Administering Avaya Aura® System Manager

Release 6.2
Issue 2.0
July 2012

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License type

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with

your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, Avaya Aura® System Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: System Manager overview

System Manager is a central management system that delivers a set of shared management services and a common console for System Manager and its components.

Important:

On the System Manager Web interface, do not use the back arrow on the top-left corner of the browser to navigate to the previous page. If you click the back arrow, the system might exhibit an inconsistent and unexpected behavior.

System Manager includes the following shared management services:

Service	Description
Bulk import and export	Provides features for bulk import and export of user profiles and global settings.
Directory synchronization	Provides features for bidirectional synchronization of user attributes from System Manager to the LDAP directory server.
Elements	Provides features by individual components of System Manager. Some links also provide access to generic features of System Manager, most of the links provide access to features provided by different components of System Manager.
Events	Provides features for administering alarms and logs generated by System Manager and other components of System Manager. Serviceability agent sends alarms and logs to SAL Gateway and System Manager, which in turn forwards the alarms and logs to the Avaya Data Center. You can view and change the status of alarms. You can view logs and harvest logs for System Manager and its components and manage loggers and appender.
Groups & Roles	Provides features for administering groups and roles. You can create and manage groups, roles, and permissions.
Licenses	Provides features for administering licenses for individual components of Avaya Aura® Unified Communication System.
Routing	Provides features for managing routing policies. You can create and manage routing applications that include Domains, Adaptations, SIP Entities, Entity Links, Time Ranges, Policies, Dial Patterns, and Regular Expressions to manage your network configuration.
Security	Provides features for configuring the certificate authority.
System Manager Data	Provides features for:

Service	Description
	• Backing up and restoring System Manager configuration data. • Monitoring and scheduling jobs. • Replicating data from remote nodes. • Configuring data retention settings and profiles for various services that System Manager provides.
Users	Provides features to administer users, shared address, public contact list, and system presence access control list information. You can: • Associate the user profiles with groups, roles, and communication profiles. • Create a contact list. • Add an address and private contacts for the user.

What is new in this release

Avaya Aura® System Manager 6.2 supports the following features and enhancements:

- Validation tool to replicate the System Manager data to other element nodes or the slave nodes
- Single role based access control for System Manager
- User Management Web services
- Single User Management interface
- **Localized Names** and **Phone Details** sections in User Management
- CS1000 Station Profile, CallPilot Messaging Profile, and B5800 Branch Gateway Profile in the Communication Profile tab, User Management screens
- Remote serviceability agents to forward logs and alarms
- Bidirectional synchronization of user attributes between System Manager and the LDAP directory server
- Manual and automatic renewal of identity certificates
- Support for Avaya Aura® Messaging 6.1
- Support for CMM 6.2
- Support for 250,000 users and 100,000 SIP Endpoints
- The following set types in Endpoint Management and User Management:

9608	9621SIP

9611	9641SIP
9621	9611SIP
9641	9608SIPCC
9404 DCP	9611SIPCC
9408 DCP	9621SIPCC
9608SIP	9641SIPCC

Note:

For 9621, 9621SIP, and 9621SIPCC set types, System Manager does not support the **Button Modules** tab in Endpoint Management.

- Use of the new 96x1SIPCC endpoint type

Note:

Administration of 16CC and 4620SIPCC set types are blocked.

- Change in user interface label in Vector Directory Number from **Reporting for PC Predictive Calls?** to **Reporting for PC or POM Calls?**
- Up to 4000 entries in IP Network Map
- The following client browsers to access System Manager and the stand-alone WebLM server:
  - Internet Explorer 7.x and 8.x
  - Firefox 3.5 and 3.6
- **UDP Groups** in **Communication Manager** > **Systems**. Includes support from Group and Lookup Service (GLS), Role Based Access Control (RBAC), and Runtime Topology System (RTS).
- **Clear AMW all** in **Maintenance** in Endpoint Management
- Duplicate endpoints in Endpoint Management
- **Enable Notifications** in **Inventory** > **Manage Elements**
- The following new fields:
  - **MOC Control** in **Class Of Service**
  - **Voice Mail Number** in **Feature Options** in Endpoint Management
  - **Call Origin** in **Vector Directory Number**
  - **Auto Abbreviated/Delayed Transition**, **Enhanced Call Pickup Delay Timer**, and **Audible Notification** in System Parameters Features
- Support for upgrading B5800 devices using the **Upgrade Management** feature - Upgrade Manager checks the software version currently in use with regards to the latest versions

available from Avaya. Upgrade Management also recommends updates for enhanced features, when a newer software version is available.

- Change in following UI labels in **Templates**:
  - **Agent** to **CM Agent**
  - **Endpoint** to **CM Endpoint**
- Upgrade of CM Agent and CM Endpoint templates in Template Management
- **B5800 Branch Gateway Manager** under **Elements**. Use this feature to:
  - Manage system configuration data under **System Configuration**
  - Manage security configuration data under **Security Configuration**
  - Perform backup and restore tasks of B5800 Branch Gateway device configuration under **Backup**, which includes system configuration data, security data, and user data
- Manage **B5800 Endpoint** and **B5800 System Configuration** templates in Template Management. In **B5800 System Configuration**, you can manage the .WAV and .C11 audio files through **Manage Audio**.
- **B5800 Branch Gateway** in **Type** in Discovery Management
- **B5800** and **B5800L** values in **Device Type** under the Attributes tab in RTS
- Ability to manage 2,000 B5800 Branch Gateway devices
- Bulk import and export of B5800 Branch Gateway users in User Management
- Create groups of B5800 Branch Gateway devices in Groups Management
- Create roles to gain access to B5800 Branch Gateway devices in role based access control

Log on to System Manager

Logging on to the System Manager Web interface

The System Manager Web interface is the main interface of Avaya Aura® System Manager. To perform any tasks, you must log on to the System Manager Web Console.

Before you begin

Obtain a user account to log on to the System Manager Web interface. If you do not have a user account, contact your system administrator to create your account.

Procedure

1. On the Web browser, enter the System Manager URL `https://<Fully Qualified Domain Name>/SMGR`.
2. In the **User ID** field, enter the user name.
3. In the **Password** field, enter the password.
4. Click **Log On**.

   The system validates the username and password with the System Manager user account. Depending on the validity, the system displays one of the following screens:

   - If the username and password match, the system displays the System Manager home page with the System Manager *version_number*. The System Manager home page displays the navigation menu. The menu provides access to shared services to perform various operations that System Manager supports. The tasks you can perform depends on your user role.
   - If the username and password does not match, System Manager displays an error message and prompts you to re-enter the user name and password.

Log-in information for users with user name *admin*

This log-in information applies only to users with log-on name admin.

- After installation, when you log on for the first time to System Manager, enter `admin123` as the default password.

  The system displays the Forced Change Password page. The Forced Change Password page does not contain the **Cancel** button. You must change the password when you log on using the default password.
- After an upgrade, when you log on to System Manager, you must reset the password.
- If you access System Manager using the IP address, and you log on as admin for the first time, to change the password manually, use the **Change Password** link.

Note:

The password must contain a combination of alphanumeric and special characters. For more information about the password strength policy, see Password strength policy enforcement on page 24.

Password and security policies for all administrators

Password aging policy enforcement

The password aging policy has the following time-based password thresholds:

- Minimum password age
- Password expiration warning
- Password expiration

A network administrator configures the password threshold in number of days.

The following table describes the impact when the password aging policy threshold expires after the user logs on to System Manager.

Password threshold	What occurs when the threshold expires
Minimum password age	You cannot change the password until the minimum password age has been reached. For example, you cannot change the password with in three days after the last change was made.
Password expiration warning	You receive a password expiration warning when the password is about to expire and before the password expires.
Password expiration period	You are forced to change the password after the threshold for the password expires and before the threshold to disable the account. The password remains locked until the network administrator resets the password.

Password strength policy enforcement

A password must contain a combination of alphanumeric and special characters as defined by the network administrator. The password strength policy enforces the following constraints:

- Passwords must have a total character length from 6 to 25. The default is eight.
- Passwords are not required to have a minimum character type. However, the default is one lower- and upper case character, one numeric character, and one special character, such as exclamation mark (!). The sum cannot exceed the minimum total length.

After you enable the password strength policy, ensure that the password meets the following standards:

- Password must not contain a character repeated more than twice consecutively.
- Passwords must not be your user ID, in forward or reverse order.

If a password does not meet the standard, the system rejects the password.

Note:

You can disable the password strength policy.

Password history policy enforcement

The password history policy verifies that a password is new. The previous blocked passwords can range from 1 to 99. The default is six.

Password lockout policy enforcement

The lockout policy provides a limit for the number of unsuccessful attempts you can make to access System Manager. The system locks System Manager for the user after a specified number of logon attempts. By default, if the consecutive attempts occur within a ten-minute period, the user is locked out for two minutes after five unsuccessful attempts.

Inactive session termination policy

By default, the system suspends a user session after 30 minutes of inactivity. When the session becomes inactive, to access System Manager, the user must log on to System Manager again.

Logon warning banner

System Manager provides the text for the logon warning banner that a network administrator can change.

Configuring the UCM services

Procedure

1. On the System Manager console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR**.
3. Click **Common Console**.
4. On the View Profile: Common Console page, set the **UCM Configured** field to **true**.
5. Click **Done**.
   The system displays the links for the UCM services in the home page. Click on the relevant links to launch UCM.

Editing password policies

Before you begin

- Configure the UCM services. For more information, see Configuring the UCM services on page 26.
- To make the UCM services available, log out from System Manager and log in again.

About this task

Using this procedure administrators can edit the password settings.

Procedure

1. On the System Manager Web Console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Policies**.
3. In the Password Policy section, click **Edit**.
4. Edit the required fields on the Password Policy page.
5. Click **Save**.
   To undo your changes and return to the previous page, click **Cancel**.

   Important:

   The system displays an invalid logon message in the following scenarios:

   - If you use a disabled account to log on.
   - If the password is invalid.

- If the maximum number of failed logon attempts limit reaches.
- If the password expires.

For each scenario, the system responds with a message that invalid logon credentials are used. You must contact the network administrator for more information on password policies.

Related topics:

Password policies field descriptions on page 28

Editing Session Properties

Before you begin

- Configure the UCM services. For more information, see Configuring the UCM services on page 26.
- To make the UCM services available, log out from System Manager and log in again.

Procedure

1. On the System Manager Web Console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Policies**.
3. On the Policies page, in the Session Properties section, click **Edit**.
4. On the Session Properties page, edit the required fields.
5. Click **Save**.

Related topics:

Session Properties field descriptions on page 30

Security settings

System Manager provides a customizable logon banner that appears when a user logs on to the system. The customizable banner is intended for use by customers with security policies that require network equipment to display a specific message to users when they log on.

Editing the login warning banner

Before you begin

- Configure the UCM services. For more information, see Configuring the UCM services on page 26.
- To make the UCM services available, log out from System Manager and log in again.

Procedure

1. On the System Manager Web Console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Policies**.
3. On the Policies page, in the Security Settings section, click **Edit**.
4. On the Security Settings page, edit the text as required in the Login Warning Banner text area.

   Note:

   The maximum number of characters allowed is 2500.
5. Click **Save**.

Password policies field descriptions

This page is applicable only for users with the user name “admin”.

Aging section

Name	Description
Enforce password aging policies	Select the check box to enforce the aging policies.
Enable expired password change	Select the check box to allow users to change password after it expires.
Expiration period	Specifies the maximum allowable days to maintain the password. Default value is 90. You can enter values from 1 to 365.
Expiration warning	Sends a warning to the user if the password is about to expire. You can type in any value from 1 to 15. The default is 7.

Name	Description
Minimum age	Specifies the minimum allowable days for password age. You can type a number from 0 to 7. The default is 3. Ensure that the number for the expiration period is greater than the minimum password age number.

History section

Name	Description
History	Select this check box to enforce policies against previously used passwords.
Previous passwords blocked	Specifies the number of passwords the system maintains in the history. You cannot reset your password to these values. The default is 6.

Strength section

Name	Description
Strength	Select the check box to enforce password content standards.
Minimum Total Length	Specifies the minimum number of characters required for the password. The default value is 8. You can set the value from 6 to 25.
Minimum by character Type: Lower case	Specifies the minimum number of lower case characters required in the password. Default value is 1.
Minimum by character Type: Upper case	Specifies the minimum number of upper case characters required in the password. Default value is 1.
Minimum by character Type: Numeric case	Specifies the minimum number of numeric characters required in the password. Default value is 1.
Minimum by character Type: Special case	Specifies the minimum number of special characters required in the password. Default value is 1.

Lockout section

Name	Description
Lockout	Select the check box to enforce lockout after failed login attempts.

Name	Description
Consecutive Invalid Login Attempts	Specifies the number of failed attempts before lockout. You can set values from 1 to 20 attempts. Default value is 3.
Interval for Consecutive Invalid Login Attempts	Time interval in minutes between invalid login attempts. You can set values from 0 to 120 minutes. Default value is 10 minutes.
Lockout Time	Specifies the number of minutes the account is locked after invalid login attempts. You can set values from 0 to 120 minutes. Default value is 2 minutes.

Button	Description
Save	Saves all your entries in the Edit Password Policies page.
Cancel	Ignores your changes and takes you back to the previous page.

Session Properties field descriptions

Name	Description
Maximum Session Time	Specifies the maximum time a session can remain active. Type any value from 0 to 1440.
Maximum Idle Time	Specifies the maximum time a session can remain idle. Type any value between 0 to 1440. **Note:** The maximum idle time cannot exceed the maximum session time.

Button	Description
Save	Saves your changes in the Session Properties page.
Cancel	Ignores your changes and takes you to the previous page.

Chapter 2: Directory synchronization

Directory synchronization overview

System Manager integrates with number of Lightweight Directory Access Protocol (LDAP) directory servers to provide the following functions:

- Synchronize users from the LDAP directory server to System Manager User Management.
- Bi-directional synchronization of user attributes from System Manager to the LDAP directory server.

LDAP supports the following directory servers for synchronization:

- Active Directory 2003
- Active Directory 2008
- OpenLDAP 2.4.21
- IBM Domino 7.0
- Novell eDirectory 8.8
- SunOne Directory/Java System Directory 6.3

The Directory Synchronization Engine runs on demand from the System Manager user Interface. You can also schedule data synchronization to and from the enterprise directory. During the synchronization of information to the enterprise directory server, System Manager modifies the data of users stored in the LDAP directory server.

You can configure bi-directional attribute mappings through the System Manager Directory Synchronization user interface. Bi-directional synchronization does not synchronize the user in the LDAP directory sync created from the System Manager user interface or created using the System Manager bulk import feature. Bi-directional synchronization only synchronizes the attributes of the user already synchronized from the LDAP directory server.

Results expected during the synchronization from the LDAP directory server to System Manager

You can expect the following results when you run the directory synchronization job manually or after the system runs the scheduled job.

Input	Provided	Expected result
You create a new user in the LDAP directory server.	The user is a part of the filter criteria.	The system synchronizes the user in System Manager.
You update the attributes of the user in the LDAP directory server.	The system adds the attributes in the mappings for that data source.	The system updates the user attributes in System Manager.
You delete a user in the LDAP directory server.	The system selects the **Allow Deletion** check box for the data source.	The system permanently deletes the user in System Manager.

Results expected during the synchronization from System Manager to the LDAP directory server

You can expect the following results when you run the directory synchronization job manually or after the system runs the scheduled job.

Input	Provided	Expected result
You update the user attributes synchronized from LDAP directory server in System Manager.	The system adds the attributes in the mappings for that datasource and the mapping synchronizes from System Manager to the LDAP directory server.	The system updates the user attributes in the LDAP directory server.

Limitations in synchronization of LDAP directory server

This section lists the limitations to the directory synchronization solution provided inSystem Manager 6.2.

You can expect the following results when you run the directory synchronization job manually or after the system runs the scheduled job.

Table 1: Synchronization from the LDAP directory server to System Manager

Input	Expected result
Synchronize users from multiple trees in the LDAP directory server.	The system does not support this using one datasource creation. As an administrator you must create two datasources with different BaseDN. The name of the datasource must be different.
Synchronize users from multiple LDAP directory servers.	Create different datasource for each directory server. The system supports authentication only one directory server.
As an administrator, modify the user attributes synchronized by the LDAP directory server.	If you add the attributes in mappings for the datasource, the system overwrites the attributes from the synchronization job.
Synchronize extensions, stations, or SIP handles using directory synchronization.	The synchronization does not happen because the Directory Synchronization feature does not support synchronization of dial-plan or SIP handles.

Table 2: Synchronization from System Manager to the LDAP server

Input	Expected result
Create a new user in System Manager using the user interface or by bulk-Import operation.	The system does not synchronize the user in the LDAP Directory Server.
Update the user attributes synchronized from the LDAP Directory Server in System Manager.	If you add the attributes in mappings for the datasource, the attributes are updated in the LDAP Directory Server. Only optional attributes can be synchronized from System Manager to the LDAP Directory Server.
Delete users in System Manager.	The system does not delete the user from the LDAP Directory Server. The Directory Synchronization feature does not support soft deletion or permanent deletion of the user from the LDAP Directory Server. The system synchronizes the user in System Manager even after you permanently delete the user.

Adding a synchronization datasource

Procedure

1. On the System Manager Web Console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Datasources** tab.
4. Click **New**.
5. On the New User Synchronization Datasource page, complete the fields in the Directory Parameters section.
6. Click **Test Connection**.

   If the connection fails, the system displays an External directory error message.

   If the connection is successful, the system displays a status icon. To view the message, click the status icon.
7. If the connection is successful, map the attributes in System Manager. The system displays five mandatory attributes that are grayed out.

   To add additional attributes, click **Add Mapping**.

   You can use any appropriate LDAP attribute to synchronize in System Manager. Ensure that the attributes mentioned for LDAP contain valid values; otherwise the synchronization fails.
8. Click **Save**.

   Note:

   To bi-directionally synchronize the data in the LDAP directory with System Manager, select the two-way arrow icon in the **Attribute Parameters** section.

   While specifying the attribute mapping, the right-arrow specifies synchronization from the LDAP server to System Manager and the left-arrow specifies the synchronization from System Manager to the LDAP server.

Related topics:

User synchronization datasource field descriptions on page 36

Editing a synchronization datasource

Procedure

1. On the System Manager Web Console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, in the **Synchronization Datasources** tab, select the record you want to edit.
4. Click **Edit**.
5. Edit the required fields on the Edit Synchronization Datasource page.
6. Click **Save**.

Related topics:

User synchronization datasource field descriptions on page 36

Deleting a synchronization datasource

Procedure

1. On the System Manager Web Console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, in the **Synchronization Datasources** tab, select the record you want to delete.
4. Click **Delete**.

Note:

If you synchronize a user using the datasource to be deleted, the delete fails. The system displays the following message: “Data Source <Datasource Name> cannot be deleted as at least one enterprise CsUser references it”.

User synchronization datasource field descriptions

Directory Parameters section

Field	Example Values	Description
Datasource Name	Win2K8AD	You can add any name to identify an active directory. You might require it later to create a sync job.
Host	148.147.163.131	IP Address or Host name of the directory server you synchronize users with.
Principal	CN=Administrator,CN=Users,DC=pansv8,DC=platform,DC=avaya,DC=com	User name of the Active Directory which has write permissions to create or update users.
Password	<password>	Password of the user mentioned above to connect to Active Directory.
Port	389	Port number of the Active Directory on which the active directory is accessible. The default value is 389.
Base Distinguished Name	CN=Users,DC=pansv8,DC=platform,DC=avaya,DC=com	The Base DN is an element that works in conjunction with the search scope. It's the tree from where you want users to be synchronized.
LDAP User Schema	inetOrgPerson	The schema defines object classes. The object class definitions define the list of attributes that must contain values and the list of attributes which might contain values. This might differ depending on your Active Directory. The default value is inetOrgPerson.
Search Filter	(cn=Alex*)	A search filter provides a mechanism for defining the criteria for matching entries in an LDAP search operation.
Use SSL	False (unchecked)	Select this check box to use SSL to connect to Active Directory. For information on setting up the SSL connection, see Adding trusted certificates on page 952.
Allow Deletions	False (unchecked)	Select this check box to delete an already synchronized user deleted from the Active Directory.

Attribute Parameters section

LDAP Attribute	System Manager Attribute	Description
objectGUID	sourceUserKey	The attribute that uniquely define a user.
userPrincipalName	loginName	The attribute that you can use as login name in System Manager.
sn	surname	The attribute which defines the last name for the user.
givenName	givenName	The attribute that you can use as the given name.
displayName	displayName	The attribute that you can use as the display name.
middleName	middleName	The attribute that you can use as middle name.
mail	email	The attribute that you can use as the communication profile handle.
postalCode	postalCode	The attribute that you can use as the postal code for user address. The system creates the address for the user with the name as “Registered_User_Address”.
streetAddress	streetAddress	The attribute you can use as the postal code for user address. The system creates the address for the user with name as “Registered_User_Address”
preferredLanguage	preferredLanguage	The attribute you can use as the preferred language for the user. The application supports only the G13 languages. Ensure that the LDAP attribute mapping to preferredLanguage is in the format LanguageCode_CountryCode. The following list gives the format for all the G13

LDAP Attribute	System Manager Attribute	Description
		languages that are supported in the preferredLanguage attribute: • English (United States) - en_US • Chinese (Simplified) - zh_CN • Japanese (Japan) - ja_JP • Korean (Korea) - ko_KR • French (France) - fr_FR • German (Germany) - de_DE • Italian (Italy) - it_IT • Russian (Russia) - ru_RU • English (United Kingdom) - en_GB • Spanish (Mexico) - es_MX • Portugese (Brazil) - pt_BR • French (Canada) - fr_CA • English (Canada) - en_CA
mail	otherEmail	The attribute that you can use as the secondary e-mail.
roomNumber	room	The attribute that you can use as a room number for user address. The system creates the address for the user with the name as “Registered_User_Address”.
co	country	The attribute that you can as the country for the user address. The system creates the address for the user with the name as “Registered_User_Address”.
telephoneNumber	businessPhone	The attribute that you can use as the business telephone number for the user phone details under the

LDAP Attribute	System Manager Attribute	Description
		“Registered_User_Address” address.
otherTelephone	otherBusinessPhone	The attribute that you can use as the secondary business telephone number for the user phone details under the “Registered_User_Address” address.
facsimileTelephoneNumber	fax	The attribute that you can use as the fax number for the user phone details under the “Registered_User_Address” address.
homePhone	homePhone	The attribute that you can use as the residential phone number for the user phone details under the “Registered_User_Address” address.
otherHomePhone	otherHomePhone	The attribute that you can use as the secondary residential phone number for the user phone details under the “Registered_User_Address” address.
mobile	mobilePhone	The attribute that you can use as the mobile phone number for the user phone details under the “Registered_User_Address” address.
otherMobilePhone	otherMobilePhone	The attribute that you can use as the secondary mobile phone number for the user phone details under the “Registered_User_Address” address.
pager	pager	The attribute that you can use as the pager number for the user phone details under the “Registered_User_Address” address.

LDAP Attribute	System Manager Attribute	Description
otherPager	otherPager	The attribute that you can use as the secondary pager number for the user phone details under the “Registered_User_Address” address.
givenName	preferredGivenName	The attribute that you can use as the preferred given name for the user.
organization	organization	The attribute that you can use as the organization the user belongs to.
department	department	The attribute that you can use as the department the user belongs to.
employeeID	employeeNo	The attribute that you can use as the employee ID or number of the user.
st	stateOrProvince	The attribute that you can use as the state or the province for the user address. The system creates the address for the user with the name as “Registered_User_Address”.
l	localityName	The attribute that you can use as the locality name for the user address. The system creates the address for the user with the name as “Registered_User_Address”.
displayName	localizedName	The attribute that you can use as the localized name for the user in different languages. **Note:** The LDAP attribute mapping to localizedName must be in the format: “Locale.Name”. For example, if the locale is English and user name is Alex, then the value for

LDAP Attribute	System Manager Attribute	Description
		displayName must be `en.Alex`.

Button	Description
Save	Adds a new datasource or saves the edits that you make.
Cancel	Cancels your action and takes you to the previous page.

Note:

You must select the text or binary values from the drop-down list beside the mappings. If you select binary from the drop-down list, the value is encoded and is displayed as an encoded value in the UI.

Related topics:

Editing a synchronization datasource on page 35

Creating a user synchronization job

Procedure

1. On the System Manager Web Console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Active Synchronization Jobs** tab.
4. Click **Create New Job**.
5. Select a datasource name for the datasource that you want to synchronize.
6. Do one of the following:
   a. Select **Run Job** to execute the job immediately.
   b. Select **Schedule job for future execution** to schedule the job at a later time.

Note:

You can delete a job that is scheduled to execute in the future.

Related topics:

User active synchronization job field descriptions on page 43

Scheduling a user synchronization job

Procedure

1. On the System Manager Web Console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Active Synchronization Jobs** tab.
4. Click **Create New Job**.
5. Select the **Datasource Name** for which you want to schedule a job.
6. Select the **Schedule job for future execution** checkbox.
7. Select a **Date** when you want to execute the job.
8. Select the **Time** when you want to execute the job.
9. Select the appropriate **Time Zone** from the drop down list.
10. Select the **Repeat Job Execution** checkbox if you want to repeat the job execution.
11. Select the recurring interval in minutes, hours, days, weeks or months.
12. Click **Schedule job for future execution**.

Deleting a user synchronization job

Procedure

1. On the System Manager Web Console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, in the **Synchronization Job History** tab, choose the job you want to delete.
4. Click **Delete Job**.

   The system deletes the job without any confirmation.

Note:

You can delete a job that is scheduled to run in the future.

User active synchronization job field descriptions

Name	Description
Datasource Name	Specifies the name of the datasource.
Schedule job for future execution	Schedules a user synchronization job.
Date	Specifies the date when you want to schedule the job.
Time	Specifies the time when you want to schedule the job.
Time Zone	Select the time zone closest to your location.

Button	Description
Run Job	Runs the user synchronization job you specify.
Schedule job for future execution	This button appears only when you select the **Schedule job for future execution** check box. Schedules a user synchronization job.
Cancel	Cancels the synchronization and takes you to the previous page.

Synchronization job history

The **Synchronization Job History** tab displays the history of the jobs created for user synchronization and the result of each job execution. You can delete the entry a user synchronization job result from the list using the **Delete Job** link.

Related topics:

Synchronization job history field descriptions on page 44

Synchronization job history field descriptions

Name	Description
Start Time	Specifies the start time when a user synchronization job was started.
End Time	Specifies the time when a user synchronization job was completed.
Name	Specifies the datasource name for which the user synchronization job was executed.
Status	Displays the status of the user synchronization job.
Job Result	Contains the **View Job Summary** link that takes you to the user synchronization job execution result details page.
Action	Contains the **Delete Job** link for deleting a user synchronization job execution result.

Viewing Job Summary

Procedure

1. On the System Manager Web Console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Job History** tab.
4. Click the **View Job Summary** link in the **Job Result** column.

Related topics:

Viewing Job Summary field descriptions on page 45

Viewing Job Summary field descriptions

Name	Description
Datasource Name	Specifies the datasource name for which the user synchronization job was executed.
End Time	Specifies the time when the user synchronization job was completed.
Job Results	Specifies the user synchronization job execution result details.
Added	Specifies the number of users added to the system after the job execution. For a non-zero count, the system displays an expand/collapse icon. Click this icon to show/hide the details of user entries that were added.
Modified	Specifies the number of users modified after the job execution. For a non-zero count, the system displays an expand/collapse icon. Click this icon to show/hide the details of modified user entries.
Deleted	Specifies the number of users deleted after the job execution. For a non-zero count, the system displays an expand/collapse icon. Click this icon to show/hide the details of deleted user entries.
Unchanged	Specifies the number of users that were modified after to the job execution.
Failed	Specifies the number of user records that could not be synchronized due to some errors. For a non-zero count, the system displays an expand/collapse icon. Click this to show/hide the details of user entries for which synchronization failed.
Total records processed	Specifies the total number of user records that were processed during the job execution.

Button	Description
Back	Takes you to the previous page.

Chapter 3: Managing groups and roles for resources

Managing groups

Group management

Group and Lookup Service (GLS) in System Manager is a shared service that provides group administration and lookup service for managed resources. GLS encapsulates the mechanisms for creating, modifying, searching, and deleting groups and group memberships.

Using GLS, you can create a separate set of permissions and assign the permissions to different users based on designations of users. You can distribute different roles to the administrators and allow the administrators to perform only limited tasks on the System Manager console. For example, a user with the role of an auditor can only audit limited functionality of the system. An auditor cannot perform any administrative changes on the System Manager console.

GLS supports group administration for common resources shared across elements such as, roles and users, as well as element-specific resources that are not shared. GLS also supports bulk import of groups and group memberships. Using GLS, you can group resources any way that works best for the business, such as, organizing resources by location, organization, and function.

GLS maintains a repository of groups and memberships from System Manager and other applications that use this service. GLS synchronizes the resources with other Avaya applications and services that are managing these resources. GLS maintains resource IDs and their group memberships. However, GLS does not maintain resource attributes. Through GLS you can search one or more resources based on their attribute values and obtain resource attributes for one or a set of resources.

You can perform the following operations using GLS:

- Create groups
- View and modify groups
- Create duplicate groups by copying properties of existing groups

- Assign and remove resources for groups
- Delete groups
- Synchronize groups

As a shared service, GLS reduces the time and effort involved in defining groups of managed resources that more than one application or service requires. You can use the group of resources to assign permissions through RBAC.

Viewing groups

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, select a group and perform one of the following steps:
   - If the selected group is a selection-based group member, then click **View**.
   - If the selected group is a query-based group, then on the View group page, click **Execute query**.

   The system displays the View group page with the selected group details and the resources assigned to the group.

Related topics:

View group field descriptions on page 58

Creating groups

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, perform one of the following steps:
   - To create a group, click **New**.
   - To create a subgroup under a group or a subgroup, select a group or a subgroup and click **New**.
4. On the Create group page, enter the appropriate information.

5. Click **Commit** to create the new group.

Related topics:

New group field descriptions on page 60

Modifying groups

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, select a group.
4. Click **Edit** or click **View** > **Edit**.
5. On the Edit group page, enter the appropriate information.
6. Click **Commit** to save the changes to the database.

Related topics:

Edit group field descriptions on page 62

Creating duplicate groups

You can use this feature to create a duplicate group by copying the properties of an existing group. When you create a duplicate group, the system copies all the information from the existing group to the new group.

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, select a group.
4. Click **Duplicate**.
5. On the Duplicate group page, perform any one of the following steps:
   - To create a duplicate group at root level, click **Root** .
   - To create a duplicate group under a group or a subgroup, select a group or a subgroup, and click **Selected group**.

   To view the subgroups in a group, click **+**.

The system displays the duplicate group on the Group management page as copy of the parent group (the parent group from which the group is created).

Note:

Use the edit functionality to change the properties of this group.

Related topics:

Duplicate group field descriptions on page 64

Deleting groups

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, select the groups you want to delete.
4. Click **Delete**.
5. On the Delete group confirmation page, click **Delete**.

Related topics:

Delete group confirmation field descriptions on page 64

Moving groups

You can move a group from one group to an another group or to the root level. You can also move a group from the root level to an another group.

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, select a group.
4. Click **More Actions** > **Move**.
5. On the Move group page, perform one of the following steps:
   - To move a group to the root level, click **Root**.

- To move a group to another group or a subgroup, select the group or the subgroup, and click **Selected group**.

To view the subgroups in a group, click **+**.

Related topics:

Move group field descriptions on page 65

Synchronizing resources for a resource type

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, click **More Actions** > **Sync**.
4. On the Resource synchronization page, select the type of resources from the **Type** drop-down field.
5. Click **Sync**.

Related topics:

Resource synchronization field descriptions on page 65

Assigning resources to a group

You can assign only resources of the type that is configured for the group. The type of resource that you can assign to a group is set when you create a group. For example, if the type of resource is set to *ALL*, you can assign all types of resource to the group. If the type is set to a specific type of resource, you can only assign resources of the specific type to that group.

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page click **New**.
4. Specify a group name and select a group type.
5. Click **Assign resources**.

To assign a resource to an existing group, select the group and perform one of the following:

- Click **Edit** > **Assign resources**.
- Click **View** > **Edit** > **Assign resources**.

6. On the Resources page, select a resource.

   The Resources page displays all the resources available in the application, but you cannot select the resources that are already assigned to the group.

   You can also search for a resource using **Advance Search**.

7. Click **Add To Group**.
   The system adds the selected resources to the group.

Related topics:

Resources field descriptions on page 69

Searching for resources

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, perform one of the following:
   - Click **New** > **Assign resources**.
   - Click **Edit** > **Assign resources**.
   - Click **View** > **Edit** > **Assign resources**.
4. On the Resources page, click **Advanced Search**.
5. In the Criteria section, perform the following:
   a. Select the resource type from the **Type** drop-down field
   b. Select the search criterion from the first drop-down field.
   c. Select the operator from the second drop-down field.
   d. Enter search value in the third field.
6. If you want to add another search condition, click the **+** button.

   Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.

7. Select the **AND** or **OR** from the drop-down field.

   This option appears only when you add a search condition using the **+** button.

8. Click **Search**.

   The Resources section displays the resources matching the search criteria. If no resources match the search criteria, the Resource section displays the message `No records are found`.

Searching for resources based on group membership

About this task

You can only search resources based on group membership on the Group management page using the Advanced Search capability.

Note:

You cannot search resources based on group membership on the Resources page using the Advanced Search capability.

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, click **Advanced Search**.
4. In the **Criteria** section, select the search criterion from each of the drop-down fields.
   a. Select the search criterion from the first field.
   b. Select the operator from the second field.
   c. Enter the search value in the third field.
5. If you want to add another search condition, click the **+** button.

   Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
6. Select the **AND** or **OR** from the drop-down field.

   The system displays this option when you add a search condition using the **+** button
7. Click **Search**.

Related topics:

Resources field descriptions on page 69

Filtering groups

About this task

You can apply filter on the following three columns:

- Name
- Type
- Hierarchy

You can filter groups using one or multiple column filters.

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, click **Filter: Enable**.
4. Enter the group name in the field under the **Name** column.
5. Select the resource type from the drop-down field under the **Type** column.
6. Enter the hierarchy level under the **Hierarchy** column.

   When you enter a hierarchy level, the table displays only those groups that you have created under that level. For example, to view all the groups that you created under root, enter / as hierarchy level.
7. Perform one of the following:
   - Click **Apply**. The table displays only those groups that match the filter criteria
   - Click **Disable** to hide the column filters. This action does not clear any filter criteria that you have set.
   - Click **Clear** to clear the filter criteria.

Filtering resources

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, select a group if you are assigning a resource to an existing group.
4. Perform one of the following steps.

- Click **New** > **Assign resources**.
- Click **Edit** > **Assign resources**.
- Click **View** > **Edit** > **Assign resources**.

5. On the Resources page, click **Filter: Enable**.
6. Enter the resource name in the field under the **Name** column.

   Note:

   You can apply filter on one column or multiple columns.
7. Select the resource type from the field under the **Type** column.

   Note:

   You can apply filter on one column or multiple columns.
8. Click **Apply** .

   Note:

   To hide the column filters, click **Disable**. This action does not clear the filter criteria that you have set in the column filters.

Result

The table displays resources that match the filter criteria.

Searching groups

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group management page, click **Advanced Search**.
4. In the **Criteria** section, perform the following:
   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter the search value in the third field.

   To add a search condition, click **+** and repeat Step a through Step c listed in Step 4.

   To delete a search condition, click **-**. This button is available if more than one search condition exists.
5. Click **Search**.

The page displays the groups that match the value specified for the search criteria.

Removing assigned resources from a group

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. Perform one of the following steps:
   - If you assigned resources to the group while creating a new group, select the resources and click **Remove**.
   - Select a group and click **Edit** > **Remove**.
   - Select a group and click **View** > **Edit** > **Remove**.

Group management field descriptions

Name	Description
Select check box	Use this check box to select a group.
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description of the group.
Dynamic	The value indicates whether resource assignment for the group is dynamic or static. **Note:** You can view this column in Tree view.

Button	Description
View	Opens the View group page that allows you to see the details of the selected group.

Button	Description
Edit	Opens the Edit group page you can use to modify the information of the selected group.
New	Opens the Create group page you can use to create a new group.
Duplicate	Opens the Duplicate group page that you can use to duplicate a group to another selected group.
Delete	Deletes the selected groups.
More Actions > **Move**	Opens the Move page that you can use to move a group to another selected group.
More Actions > **Sync**	Opens the Resource sync page that you can use to synchronize resources for a resource type.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a group.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters groups based on the filter criteria.
Select: All	Selects all the groups in the table.
Select: None	Clears all the check box selections.
Refresh	Refreshes the groups information.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Criteria	Displays the following three fields: • Drop-down 1 –- The list of criteria to search groups. • Drop-down 2 – The list of operators for evaluating the expression. This list of operators depends on the type of criterion

Name	Description
	that you selected in the first drop-down field. • Field 3 – The value for the search criterion. The Group management service retrieves and displays the groups that match this value.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches group based on the specified search conditions and displays the search results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

View group field descriptions

Use this page to view a selected group. You cannot modify the information in the fields in view mode.

View group

Name	Description
Name	Unique name of the group.
Type	Group type based on the resources. The options are: • Creating the group having member of same resource type. • All – Creating the group without any restrictions on its member.
Group membership	The options are: • Query based. Use this option to create a group that contains resources that match a specific query criteria. Query-based groups can have resources only of a specific type. You can create only typed (resource type) query groups. Thus, these groups cannot have subgroups. • Selection based. Use this option to create a group that contains resources based on

Name	Description
	static assignment. These groups can have subgroups. Subgroups and parent group might have members of the same resource type or different resource types.
Description	A brief description of the group.

Button	Description
Edit	Opens the Edit group page that you can use to modify the group information.
Done	Closes the View group page and takes you to the Group management page.

Define query

The page displays the following fields when you use **Query based** option for creating group members:

Name/Button	Description
Define query	Displays the following three fields: • Drop-down 1 – The list of criteria that you can use to search resources. • Drop-down 2 – The list of operators for evaluating the expression. The list of operators depends on the type of criterion that you selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.
+	Adds a search condition row for defining a new search condition.
–	Removes a search condition.
Execute query	Runs the query and fetches resources matching the search conditions defined in the query. The page displays these resources in the **Results** section. **Note:** This button is visible only when you create a query-based group.

The page displays following fields for assigned resources.

Name	Description
Name	Name of the resource.
Type	Type of the resource.

New group field descriptions

Use this page to create a new group.

New group

Name	Description
Name	Unique name of the group.
Type	Group type based on the resources. The options are: • Creating the group having member of same resource type. • All – Creating the group without any restrictions on its member.
Group membership	The options are: • Query based. Use this option to create a group that contains resources that match a specific query criteria. Query-based groups can have resources only of a specific type. You can create only typed (resource type) query groups. Thus, these groups cannot have subgroups. • Selection based. Use this option to create a group that contains resources based on static assignment. These groups can have subgroups. Subgroups and parent group might have members of the same resource type or different resource types.
Description	A brief description of the group.

Button	Description
Assign resources	Opens the Resources page that you can use to search and assign resources to a group. **Note:** The **Assign resources** button is available only when you use the **Selection based**

Button	Description
	option for creating group members in the group.
Commit	Creates a new group with the specified configurations.
Cancel	Closes the Create group page without saving any information on the page and returns to the Group management page.

Define query

The page displays the following fields when you use the **Query based** option for creating group members.

Name/Button	Description
Define query	Displays the following three fields: • Drop-down 1 – The list of criteria that you can use to search resources. • Drop-down 2 – The list of operators for evaluating the expression. The list of operators depends on the type of criterion that you selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.
+	Adds a search condition row for defining a new search condition.
–	Removes a search condition.
Execute query	Runs the query and fetches resources matching the search conditions defined in the query. The page displays these resources in the **Results** section. **Note:** This button is visible only when you create a query-based group.
Name	Name of the resource.
Type	Type of the resource.

Assigned resources

The page displays the following fields when you use the **Selection based** option for creating group members.

Name	Description
Name	Name of the resource.
Type	Type of the resource.
Assign resources	Opens the Resources page that you can use to search and assign resources to a group.
Remove	Removes the selected resources from the list of assigned resources.

Edit group field descriptions

Use this page to modify a selected group. You cannot modify the following fields:

- Type
- Group membership

Edit group

Name	Description
Name	Unique name of the group.
Type	Group type based on the resources. The options are: • Creating the group having member of same resource type. • All – Creating the group without any restrictions on its member.
Group membership	The options are: • Query based. Use this option to create a group that contains resources that match a specific query criteria. Query-based groups can have resources only of a specific type. You can create only typed (resource type) query groups. Thus, these groups cannot have subgroups. • Selection based. Use this option to create a group that contains resources based on static assignment. These groups can have subgroups. Subgroups and parent group might have members of the same resource type or different resource types.
Description	A brief description of the group.

Button	Description
Commit	Saves the changes in the database.
Cancel	Closes the Edit group page without saving any information and returns to the Group management page.

Define query

The page displays the following fields when you use the **Query based** option for creating group members.

Name/Button	Description
Define query	Displays the following three fields: • Drop-down 1 – The list of criteria that you can use to search resources. • Drop-down 2 – The list of operators for evaluating the expression. The list of operators depends on the type of criterion that you selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.
+	Adds a search condition row for defining a new search condition.
–	Removes a search condition.
Execute query	Runs the query and fetches resources matching the search conditions defined in the query. The page displays these resources in the **Results** section. **Note:** This button is visible only when you create a query-based group.
Name	Name of the resource.
Type	Type of the resource.

Assigned resources

The page displays the following fields when you use the **Selection Based** option for creating group members.

Name	Description
Name	Name of the resource.
Type	Type of the resource.

Name	Description
Assign resources	Opens the Resources page that you can use to search and assign resources to a group.
Remove	Remove the selected resources from the list of assigned resources.

Delete group confirmation field descriptions

Use this page to delete the groups listed in the table.

Name	Description
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description of the group.
Sub-Group count	Count of sub groups in the parent group.
Resource count	Count of the resources in the group.

Button	Description
Delete	Deletes the groups listed in the table.
Cancel	Cancels the delete operation and takes you to the Group management page.

Duplicate group field descriptions

Use this page to create a duplicate group from an existing group.

Name	Description
Select	Select a group
Name	The groups under which you can create a duplicate group. Use **+** to expand a group.

Button	Description
Root	Creates a duplicate group at the root level.
Selected Group	Creates a duplicate group under the selected group.

Button	Description
Cancel	Closes the page and returns to the Group Management page.

Move group field descriptions

Use this page to move a group to another group or to root level.

Name	Description
Select	Selects a group.
Name	The groups to which you can move the selected group. Use **+** to expand a group.

Button	Description
Root	Moves the selected group to the root level.
Selected Group	Moves the selected group to the group that you selected in the **Name** column.
Cancel	Closes the Move Group page and returns to the Group Management page.

Resource synchronization field descriptions

Use this page to synchronize resources for a resource type.

Name	Description
Type	The type based on the resources it contains.
Sync	Synchronizes resources for the selected resource type and returns to the Group management page.
Cancel	Closes the Resource synchronization page and returns to Group management page.

Managing resources

Manage resources

System Manager contains different types of resources such as users, roles, and so on. You can view and filter these resources based on filter criteria. You can also add resources of the same or different types in a group.

Accessing resources

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Resources**.

Related topics:

Resources field descriptions on page 69

Assigning resources to a new group

About this task

Use this functionality to create a new group and assign resources to this group. You can choose to create the new group at root level or under an existing group.

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Resources**.
3. On the Resources page, select a resource from the Resources table or search a resource using **Advanced Search**.
4. Click **Add To New Group**.
5. Perform one of the following:
    - To add a resource to a new group at root level, perform the following steps:

i. On the Choose Parent Group page, click **Root**.

ii. On the Create Group page, enter the appropriate information.

iii. Click **Commit**.

- To add a resource to a new subgroup under a group, perform the following steps:

i. On the Choose Parent Group page, click a group.

Note:

If you want to select a subgroup of a group, click **+** and click the subgroup.

ii. Click **Selected Group**.

iii. On the Create Group page, enter the appropriate information.

iv. Click **Commit**.

Note:

The system creates the new group and assigns the selected resources. This group is added under the group that you selected on the Choose Parent Group page.

Related topics:

New group field descriptions on page 60
Resources field descriptions on page 69

Adding resources to a selected group

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Resources**.
3. Select a resource from the resource table.
   You can also click the **Advanced Search** link to search a resource.
4. Click **Add To Group** .
5. On the Choose Group page, click a group.
6. Click **Selected Group**.

The Group Management module assigns the selected resources to the selected groups on the Choose Group page.

Related topics:

Resources field descriptions on page 69

Searching for resources

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Resources**.
3. On the Resources page, click **Advanced Search**.
4. In the Criteria section, select a type of resource from the **Type** drop-down field.
5. In the Criteria section, under **Resource Attributes**, perform the following steps:
   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter search value in the third field.
6. If you want to add another search condition, click the **+** button.
   Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
7. Select the **AND** or **OR** from the drop-down field.
   This option appears when you add a search condition using the **+** button.
8. Click **Search**.
   The Resources section displays the resources matching the search criteria. If no resources match the search criteria, system displays the message `No records are found`.

Filtering resources

About this task

You can filter and view resources that meet the specified filter criteria. Applying the filters requires you to specify the filter criteria in the fields provided under columns in the table displaying the resources. The column titles are the filter criteria. You can filter resources on multiple filter criteria.

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Resources**.
3. On the Resources page, click **Filter: Enable**.
4. Enter the resource name in the field under the **Name** column.
   You may choose to apply filter on one column or multiple columns.
5. Select the resource type from the field under the **Type** column.
   You may choose to apply filter on one column or multiple columns.
6. Click **Apply** .
   To hide the column filters, click **Disable**. This action does not clear the filter criteria that you have set in the column filters.

   The table displays resources that match the filter criteria.

Resources field descriptions

Use this page to search and assign a resource to a group. You can use this page to perform the following tasks:

- Add a selected resource to a new group or to a chosen group.
- Apply filters to view only those resources that match the filter criteria.
- Define search conditions to search resources that match the search conditions.
- View details of the attributes for the selected resources.
- View group membership details for the selected resources.

The sections on this page are:

- Criteria
- Resources
- Attributes of resources
- Resource is member of following groups

Resources section

Name	Description
Select	Use this check box to select a record.
ID	Unique name of the resource. Also known as native ID of the resource

Name	Description
Type	The type based on the resources.
View Details	Displays the attributes and membership details of the selected resources on the same page.

Button	Description
Add to Group	Opens the Choose Group page. Use this page to choose a group in which you want to add the selected resource.
Add to New Group	Opens the Choose Parent Group page. Use this page to add the selected resources to a new group or to a chosen group.
Cancel	Closes the Resources page and take you to the Create Group page.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a resource.
Filter: Enable	Displays fields under the columns **ID** and **Type**. You can use them to set the filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters the resources based on the filter criteria.
Select: All	Select all the resources in the table.
Select: None	Clears the selection for the resources that you selected.
Refresh	Refreshes resource information in the table.

Attributes of Resource section

Name	Description
Name	Name of the attribute.
Value	Value assigned to the attribute for the resource.

Resource is member of following groups section

Name	Description
Name	Unique name of the group.
Type	Group type based on the resources it contains.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Type	The types based on the resources it contains.
Resource Attributes	Displays the following three fields: • Drop-down 1 - The criteria for searching a resource. The options are attributes of resources for the attribute type selected in the **Type** drop-down list. • Drop-down 2 – The list of operators for evaluating the expression. The list of operators depends on the type of attribute selected in the first drop-down list. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the resources matching the search conditions.
Close	Closes the Criteria section.
Advanced Search	Cancels the search operation and hides the **Criteria** section.

Choose Group field descriptions

Use this page to add resources to the selected groups.

Name	Description
Select	Use this option to select a group.
Name	Name of the group.
Type	Group type based on the type of resources. The options are: • Groups having members of same resource type. • All — Groups having members of any resource types.
Dynamic	Indicates whether the group uses a query to determine its members or has static members. The options are: • **True**: Indicates that group membership is not permanent. • **False**: Indicates groups with static members.
Description	A brief description of the group.

Button	Description
Expand All	Displays the subgroups of groups listed in the table.
Collapse All	Hides the subgroups of all the expanded groups.
Selected Group	Adds the resource as a member of the selected group.
Cancel	Closes the Choose Group page and takes you to the Resources page.

Choose Parent Group field descriptions

Use this page to add resources to a selected group or to a new group.

Name	Description
Select	Use this option to select a group.
Name	Name of the group.

Name	Description
Type	Group type based on the type of resources. The options are: • Groups having members of same resource type. • All — Groups having members of any resource types.
Dynamic	Indicates whether the group uses a query to determine its members or has static members. The options are: • **True**: Indicates that group membership is not permanent. • **False**: Indicates groups with static members.
Description	A brief description of the group.

Button	Description
Expand All	Displays the subgroups of groups listed in the table.
Collapse All	Hides the subgroups of all the expanded groups.
Root	Opens the New Group page. Use this page to create a new group. The selected resource is the member of this group.
Selected Group	Adds the resource as a member of the selected group.
Cancel	Closes the Choose Parent Group page and takes you to the Resources page.

Managing roles

Role Based Access Control

In System Manager, you must have permissions to perform tasks. The Role Based Access Control (RBAC) in System Manager supports two types of roles:

- built-in
- custom

Using these roles, you can access various elements with specific permission mappings.

Built-in roles are the default roles supported by System Manager. You can assign these roles to users but you cannot delete or change the permission mappings in the built-in roles. Built-in roles provide authorization to users whose roles are authorized for all the elements.

Related topics:

Built-in roles on page 74
Custom roles on page 77

Built-in roles

The following table provides the built-in roles with a description for each role:

Role	Privileges
Auditor	Gives you read-only access to observe the system. Gives you read-only access to logs, configuration information and audit files. Does not allow you to execute any command.
System Administrator	Gives you read-write access to system parameters (Example: IP addresses, upgrade software), and the ability to modify, assign, or define other roles and read/write access to create and modify logins and all other functionalities.
Avaya Services Administrator	
Avaya Services Maintenance and Support	Gives you read-only access to maintenance logs, the ability to run diagnostics and view the output of diagnostics tools. Does not allow you to execute any command that may allow you to access another host (host containment).
Backup Administrator	Gives you access to perform backups and restores.
Discovery Admin	Allows you to configure discovery parameters like SNMP version, SNMP credentials, the subnets and devices that you want to discover. You also have the rights to schedule and run a discovery operation.
End-user	Allows you to change your end-user password.
Messaging System Admin	Gives you access and permission to all the activities related to messaging or mailbox. You cannot perform any tasks related to Communication Manager as an Modular Messaging Administrator.
Presence Admin	Gives you read-write access to the Presence configuration.

Presence Auditor	Gives you read-only access to logs, configuration information and audit filesThe Auditor role does not allow to execute any command that may allow you to access another host.
Security Administrator	Gives you read-write access to create other logins, create, modify or assign roles, install ASG keys, install licenses, install PKI certificates and keys.
SIP AS Auditor	Gives you read-only access to all the SIP Foundation server management functionality.
SIP AS Security Administrator	Gives you access to the security features provided by the SIP Foundation server. For example, Security Extension.
SIP AS Administrator	Gives you read and write access to all the SIP Foundation server management functionality.
CS1000_Admin1	Provides unrestricted OAM access to most administrative functions (except security and account administration) and provisioning for all customers on all call servers and related elements. The role also includes basic diagnostic (PDT1) privileges and access to network-level services for deployment, patching, and SNMP management for CS 1000 systems. Gives you authorization to use all roles on all UCM elements with all permissions. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: Linux Base • All elements of type: Patching Manager • All elements of type: SNMP Manager As this role gives permissions to All elements of type: Linux Base, this role is not meant forusers who only require authorization to manage CS 1000 systems. The administrator must create a custom role for these users.
CS1000_Admin2	Provides unrestricted OAM access including security and account administration, and provisioning for all customers on all call server elements. The role also includes basic diagnostic (PDT1) privileges and access to network-level services for deployment, patching, SNMP, IPsec and SFTP management for CS1000 systems. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: IPSec Manager • All elements of type: Linux Base • All elements of type: Patching Manager

	• All elements of type: Secure FTP Token Manager • All elements of type: SNMP Manager As this role gives permissions to All elements of type: Linux Base, this role is not meant for users who only require authorization to manage CS 1000 systems. The administrator must create a custom role for these users.
CS1000_CLI_Registrar	Provides permission to register and unregister individual CS 1000 elements, such as Call Server, MGC, and Media Card, using the local device OAM CLI. The role has a single permission value to allow or deny a user to register or unregister an element. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Linux Base Users assigned to this role do not have CS 1000 security or Network level security privileges. This role is intended specifically for installation and repair technicians.
CS1000_PDT2	Provides full diagnostic and operating system access to all call servers. It restricts access to administrative functions and customer provisioning data unless combined with another role. You have access to the All elements of type: CS1000.
MemberRegistrar	Provides limited access. You can register new members to the primary server. You have access to the following elements: • All elements of type: IPSec Manager • All elements of type: LinuxBase The following hidden permissions are granted to the MemberRegistrar role and cannot be copied to another role. PERM_PkiAdmin: Permission to perform PKI administration operations.
NetworkAdministrator	Provides full privileges on the system. With this role, you have emergency account access to any system including situations when the primary server is down. This role authorizes you to administer all roles on all UCM elements with all permissions. It is a best practice for the administrator to create separate administrative roles for managing UCM elements and services other than UCM security policies, roles, and users. The NetworkAdministrator role should be used only to manage security. You have access to the following elements: • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: Hyperlink

	• All elements of type: IPSec Manager • All elements of type: Linux Base • All elements of type: Network Routing Service • All elements of type: Patching Manager • All elements of type: Secure FTP Token Manager • All elements of type: SNMP Manager • All elements of type: Subscriber Manager The following hidden permissions are granted to the NetworkAdministrator role and cannot be copied to another role: • PERM_QuantumSecurityAdmin: Permission to perform UCM Security Administration operations • PERM_PkiAdmin: Permission to perform PKI administration operations • PERM_AddElement: Permission to add new element instances • PERM_DeleteElement: Permission to delete element instances • PERM_EditElement: Permission to modify existing element instances
Patcher	Provides access to software maintenance functions such as patching and maintenance. You have access to the following elements: • All elements of type: Linux Base • All elements of type: Patching Manager
Service Technician	

Related topics:

Role Based Access Control on page 73
Custom roles on page 77

Custom roles

On the Roles Web page you can create a custom role that maps to specific elements and specify customized permissions for that element. You can create custom roles for any user whose role is not authorized on one or more individual elements of any element type.

You can also assign users to perform specific tasks on an element. For example, a custom role that you create for a single element can only perform specific tasks on that element. There is a specific permissions set that defines what this role allows you to do on that element.

You can also define roles that apply to how elements and element types are hierarchically arranged under user-defined groups. When you create a permission mapping against a selected group, the system takes that group into account when determining user permissions.

Related topics:

Role Based Access Control on page 73
Built-in roles on page 74

Viewing user roles

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, click a role to view the details of the role.

Related topics:

Role page field description on page 82

Adding a custom role

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, click **Add**.
4. On the Add New Role page, fill in the **Role Name** and **Role Description** fields.
5. Click **Save and Continue**.
   The system displays the Role Details page.
6. Click the **Element/Service Permissions** tab.
7. Click **Add mapping**.
8. Perform one of the following:

- Select an element to map to the role. You can select an element by the element name or by element type. Leave the **Group Name** field blank.
- To add elements for a resource type, select the group from the **Group Name** field and an element to map to the role. You can select an element by the element name or by element type. For instructions to assign resources to a group, see Assigning resources to a group on page 51.

  Ensure that you create a group using Creating groups on page 48 before you select the group.

9. Click **Next**.

   Depending on the element type that you select, you can see the appropriate Permission Mapping page.

   The Group Name selection is optional. You do not have to change the default selection of **No Group Selected**. If you do not select a Group Name, the available element types are individual elements by name, elements by type, and network service.

   If you select a group from the Group Name list, the Element and/or Network Service Name list shows only the types (not instances) of all the available elements. The title of the Permission Mapping page changes to indicate the group you select.

   On the Permission Mapping page, select the permissions you want to assign for this role. As an administrator, you can deny, modify, or view the permissions associated with a role.

10. Click **Save**.

    The system displays the Role Details page with the permissions you have chosen.

11. Click **Save** to confirm your settings.

Related topics:

Add role field descriptions on page 82
Add mapping field descriptions on page 83

Using templates for mapping permissions

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, click a role from the **Role Name** column.
4. Click the **Element/Service Permissions** tab.

5. Click **Add Mapping**.
6. Select an Element Name, for example, CS1000, from the list.
7. Click **Next**.

   The system displays the permission mapping for the element you choose.
8. You can modify the permissions by selecting or clearing check boxes. You can also select another permission set by choosing another template from the list.
9. Click **Save**.

Assigning users to a role

To assign an *admin* role to an end user, follow the instructions described in Assigning roles to a user on page 91. An end user is a user without an *admin* role.

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role.
4. On the Role Details page, click the **Assigned Users** tab.
5. To assign or edit a role to individual users, click **Select Users**.
   The system displays the Assigned Users page.

   Note:

   The system does not display the end users in the **Assigned Users** list. You assign an *admin* role to an end user from **User Management** > **Manage Users**. For instructions, see Assigning roles to a user on page 91.
6. Select the users to whom you want to assign this role.
7. Click **Save**.
   The system displays the Role Details page where you can view the permissions for the role.

Related topics:

Assigned users field descriptions on page 84

Copying permission mapping for a role

You cannot use the Copy All From feature to copy the permissions for the Network Administrator role.

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role.
4. On the Role Details page, click the **Assigned Users** tab.
5. Click **Copy All From**.
   The system displays the Permission Mapping page.
6. Select a role from the **Copy From Role** drop down list.

   Note:

   Copy From Role does not list the Network Administrator role. You cannot copy the permissions for this role.
7. Click **Copy**.
   The system displays the Role Details page.
8. Click **Save**.
   The system displays the Roles page where you can view the details of the role.

Related topics:

Permission mapping (Copy All From) field descriptions on page 84

Editing a role description

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, click the role you want to edit from the **Role Name** column.
4. On the Role Details page, edit the **Description** field as required.
5. Click **Save**.

Deleting the custom roles

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select the custom roles you want to delete.
4. Click **Delete**.
5. On the Delete Roles page, click **Delete** to proceed with the deletion.

Role page field description

Field	Description
Role Name	Name of the role that you are adding. The role name must be between 1-26 characters in length. Allowed characters are: a-z, A-Z, 0-9, -, and _..
Users	Number of users associated with the role.
Elements	Name of the element mapped to the role.
Description	A brief description of the role.

Button	Description
Add	Takes you to the Add Roles page where you can add a custom role.
Delete	Allows you to delete a custom role.
Refresh	Refreshes the roles table and updates the role details in the table.

Add role field descriptions

Field	Description
Role Name	Name of the custom role you are adding. The role name must be between 1 to 26

Field	Description
	characters in length. Allowed characters include a-z, A-Z, 0-9, and, _.
Role Description	A brief description of the role you are adding.

Button	Description
Save and Continue	Saves the role name and description and takes you to the Roles Details page.
Save	Saves the custom role in the database.
Cancel	Cancels the permission mapping and takes you back to the Roles page.
Add Mapping	Takes you to the permissions page where you can map permissions for the role.
Delete Mapping	Allows you to delete an existing permissions set.
Copy All From	Takes you to the Permission Mapping page where you can copy an existing permission set.

Add mapping field descriptions

Field	Description
Group Name	Name of the group you want to map to the role. Select an option from the drop down list. This is an optional field.
Element and/or Network Service Name	Specifies the elements that are available. If you choose a group, this drop down list will contain only the element types and not instance.

Button	Description
Next	Saves your changes in this page and takes you to the Permission Mapping page.
Cancel	Cancels your selection and takes you to the Roles Details page.

Assigned users field descriptions

Name	Description
User Name	Name of the user you assign to the role.
Full Name	The full name of the user who is assigned to the role.
Type	-

Button	Description
Save	Assigns the users you select to the role.
Cancel	Cancels your action and takes you to the Role Details page.

Permission mapping (Copy All From) field descriptions

Field	Description
Copy from Role	Specifies the role from where you can copy all the permission mappings for the element or service.

Button	Description
Copy	Copies the permission mapping for your custom role.
Cancel	Cancels the copy action and takes you to the Role Details page.

Chapter 4: Managing users

Managing users

Manage users, public contacts, and shared address

Manage users

User Profile Management (UPM) is a shared service that users can gain access using the System Manager Web Console. UPM supports a logically centralized data store. Applications can gain access to this data store and obtain the user information that applications need. Administrators or end users do not need to enter user information for each application.

UPM provides administrators with mechanisms to:

- Administer of all user attributes, contact information, group membership, and role assignment, as well as product-specific user data.
- For each product, extend the underlying user model for product-specific properties, attributes, and any relationship between the attributes.
- Manage specific aspects of user data such as modifying a user name or address.

Using UPM, you can:

- Add user profiles.
- View, modify, and delete existing user profiles.
- Assign or remove permissions, roles, groups, addresses, and contacts for users.
- Add and modify the communication profile of users.
- Bulk import users and their attributes, public contact, shared addresses from an XML file.
- Bulk export users and their attributes to an XML file.
- Search users.

UPM uses data synchronization to achieve a single-point user administration. UPM synchronizes a user data event that is generated at the application level with the central user space and other connected applications. If an enterprise directory is connected, then UPM maintains synchronization at the enterprise level. UPM directly adjusts to the changes that occur in the enterprise directory, specifically additions, deletions, and modifications. For more information, see Directory synchronization overview on page 31.

Roles based access control (RBAC) applies to UPM such that the user role determines the access to user level and access to administrative tasks. Users with log-in privileges must have certain permissions to add, modify, and delete user accounts on the management console.

Manage public contacts

As an administrator, you can define public contacts of users in System Manager for an enterprise. You can share the public contacts by all the users in System Manager.

Manage shared address

You can manage the shared address of the users in the enterprise. All users in the enterprise share the common addresses. As an administrator, you can create a new shared address, modify and delete an existing shared address.

Viewing details of a user

Before you begin

You require appropriate permissions.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user.
4. To view details of the selected user account, click **View**.

Note:

You can only view details of one user account at a time.

Related topics:

User Profile View field descriptions on page 335

Modifying user accounts

You must have permission to modify the user details. If you select a user for which you do not have the permission to modify the details, the system does not display the **Edit** button.

Before you begin

You require appropriate permissions.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.

2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user.

   Note:

   At one time, you can edit only one user account.
4. To edit a user account, perform one of the following procedures:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. On the User Profile Edit page, modify the required information.
6. Perform one of the following procedures:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page for making further modifications, **Commit & Continue**.

Related topics:

User Profile Edit field descriptions on page 346

Creating a new user profile

Before you begin

You require appropriate permissions.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **New**.
4. On the New User Profile page, enter the appropriate information.
5. Perform one of the following procedures:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page for making further modifications, **Commit & Continue**.

   The field names marked with an asterisk (*) are mandatory fields. Before you click **Commit**, ensure that all the mandatory fields have valid information.

Important:

The names of Communication Manager systems that are undergoing synchronization does not appear in the **System** drop-down in the **Communication Profile** > **CM Endpoint Profile** section.

- For Firefox, the system displays the status of the Communication Manager systems that are undergoing synchronization as disabled. The Communication Manager systems are available only after the synchronization is complete. To view the Communication Manager systems, you must relaunch the screen.
- For Internet Explorer, the system does not display the Communication Manager systems that are undergoing synchronization in the list. The Communication Manager systems are available only after the synchronization is complete.

Related topics:

New User Profile field descriptions on page 361

Creating duplicate users

You can duplicate the user details to create a new user account by copying information from an existing user account. Using the Duplicate feature, you cannot copy the confidential information, such as addresses, private contacts, contact members in the contact list, password, and log-in name of the user.

Using the Duplicate feature, you can also copy the communication profiles like CM Endpoint and Session Manager. However, you cannot copy CS 1000 Endpoint Profile or CallPilot Messaging Profile communication. You must add the CS 1000 Endpoint Profile or CallPilot Messaging Profile communication profile after you create a duplicate user.

Before you begin

You require appropriate permissions.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the user account that you want to duplicate.
4. Click **Duplicate**.
5. On the User Profile Duplicate page, enter the appropriate information.

6. Perform one of the following procedures:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page for making further modifications, **Commit & Continue**.

Creating a user on Communication Manager

Procedure

1. Create a new user profile which is a duplicate of profile 18.
2. Assign permissions to the user profile to provide access to the shell.
3. Add additional permissions, as required.
4. Create a user with this profile.
   Use this user as log-in in Manage Elements.

Removing user accounts

About this task

When you remove a user, the system marks the user as deleted and saves the user in a list of deleted users. When you delete a user, the system removes the roles associated with the user. However, the contacts, addresses, and communication profiles of the user still exist in the database. However, you can permanently remove the deleted users from the database.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select one or more users from the table, and click **Delete**.
4. On the User Delete Confirmation page, click **Delete**.

Note:

You cannot delete users with the login name *admin* from the User Management page. The system disables the **Delete** button.

Filtering users

About this task

You can apply filter to the following user information:

- Last Name
- First Name
- Display Name
- Login Name
- E164 Handle

You can apply one or more filters to view users that match the filter criteria.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **Filter: Enable**.

   The system displays the **Filter: Enable** button at the upper-right corner of the table displaying users.
4. Enter information for one or more of the following filter criteria:
   - To filter users by last name, in the **Last Name** column, enter the last name of the user.
   - To filter users by first name, in the **First Name** column, enter the name of the user.

     To filter names that start with a particular alphabet, enter the alphabet in the field. You can enter a string of alphabets to filter the names that start with the string.
   - To filter users by login name, in the **Login Name** column, enter the login name.

     To filter login names that start with a particular alphabet, enter the alphabet in the field. You can enter a string of alphabets to filter login names that start with the string.
   - To filter users by the E164 handle, in the **E164 Handle** column, enter the E164 handle of the user.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear any filter criteria that you had set.

   To clear the filter criteria, click **Clear**.

The table displays only those users that match the filter criteria.

Searching for users

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **Advanced Search** at the upper-right corner of the page.
4. In the Criteria section, do the following:
   a. In the first field, select the search criterion.
   b. In the second field, select the operator.
   c. In the third field, enter the search value.

   To add another search criterion, click **+** (plus) and repeat Step a through Step c listed in Step 4.

   To delete a search criterion, click **-** (minus) next to the search criterion. The system displays the **-** button only if more than one search criterion is available.
5. Click **Search**.

Result

The **Users** table lists the users that match the search criteria.

Assigning roles to a user

To provide access to resources, you must assign roles to user accounts.

Note:

- You can also assign roles to users using the Roles functionality in System Manager. To access Roles, on the System Manager console, click **Groups & Roles** > **Roles**.
- To assign admin role to an end user, you must use this procedure.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, perform one of the following steps:
   - To assign roles while setting up a new user account, click **New**.
   - To assign roles to an existing user, select the user and click **Edit** or **View** > **Edit**.
4. On the User Profile Edit or New User Profile page, click the **Membership** tab.
5. Click **Assign Roles**.
6. On the Assign Roles page, select the roles from the **Available Roles** section.
7. Click **Select** to assign the roles to the selected user.
8. On the User Profile Edit or New User Profile page, click **Commit** to save the changes.

   Note:

   If you assign a different role to an end user, and you do not provide a new password, the system resets the password to match the log-in name of the user. When the user logs in, the system prompts the user to change the password on the next login.

   You can also assign roles to a user by Assigning roles to multiple users on page 92.

Assigning roles to multiple users

To provide access to resources, you must assign roles to the user accounts.

Note:

- You can also assign roles to the users using the Roles service provided by System Manager. To access the Roles service, click **Groups & Roles** > **Roles**.
- To assign admin role to an end user, you must use this procedure.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the users and click **More Actions** > **Assign Roles**.
4. On the Assign Roles page, select the roles from the **Available Roles** section.
5. Click **Commit** to assign the roles to the selected users.

Removing roles from a user

About this task

You can use this feature to remove roles from a user. You must have permissions to modify the attributes of the user.

Note:

You can also assign roles to users using the Roles functionality in System Manager. To access Roles, on the System Manager console, click **Groups & Roles** > **Roles**.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To remove a role in the edit mode, select a user and click **Edit**.
   - To remove a role in the view mode, select a user and click **Edit** on the View User Profile page.
4. On the User Profile Edit page, click the **Membership** tab.
5. Select the roles you want to remove and click **UnAssign Roles**.
6. Click **Commit** to save the changes.

Assigning groups to a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To assign groups while setting up a new user account, click **New**.
   - To assign groups to an existing user, select the user and click **Edit** or **View** > **Edit**.
4. On the User Profile Edit page or the New User Profile page, click the **Membership** tab.
5. In the Group Membership section, click **Add To Group**.

6. On the Assign Groups page, select the groups from the **Available Groups** section.
7. Click **Select** to assign the groups to the user.
8. Click **Commit**.

Assigning groups to multiple users

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the users and click **More Actions** > **Add To Group**.
4. On the Assign Groups page, select the groups from the **Available Groups** section.
5. Click **Commit** to assign groups to the selected users.

Removing a user from groups

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To remove a group in the edit mode, select the user and click **Edit**.
   - To remove a group in the view mode, select the user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Membership** tab.
5. In the Group Membership section, select the groups from which you want to remove the user and click **Remove From Group**.
6. Click **Commit** to save the changes.

Viewing the deleted users

When you remove a user from the User Management page using the **Delete** option, the system removes the user temporarily and stores the user in the **Deleted Users** table. To view the temporarily deleted users, use the **Show Deleted Users** option.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.
   On the Deleted Users page, the system displays the temporarily deleted users in the Deleted Users table.

Restoring a deleted user

You can use this functionality to restore a user that you deleted using **Delete** on the User Management page.

Before you begin

Permission to restore the selected deleted user.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.
4. On the Deleted Users page, select the user you want to restore, and click **Restore**.
5. On the User Restore Confirmation page, click **Restore**.
6. On the User Profile Edit page, enter a new password in the **Password** field.
7. In the **Confirm Password** field, enter the same password that you entered in Step 5.
8. Click **Commit**.

Removing the deleted users from the database

Using this procedure, you can permanently delete a user from the database.

Before you begin

Permission to delete the selected user.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.
4. On the Deleted Users page, select the users to delete, and click **Delete**.
5. On the User Delete Confirmation page, click **Delete**.

Assigning users to roles

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Manage Roles page, select one or more user roles.
4. Click **More Actions** > **Assign Roles to Users**.
5. On the Assign Users To Roles page, select the users displayed in the **Select Users** section.
6. Click **Commit**.

Removing users from roles

Procedure

1. On the System Manager Web Console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Manage Roles page, select one or more user roles.

4. Click **More Actions** > **UnAssign Role from Users**.
5. On the UnAssign Users To Roles page, select the users displayed in the Select Users section.
6. Click **Commit**.

Managing addresses

Adding a mailing address of a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To add a mailing address while setting up a new user account, click **New** > **Identity** > **Address** > **New**.
   - To add a new mailing address for an existing user, select the user and click **Edit** > **Identity** > **Address** > **New**.
4. On the Add Address page, enter the address details.
5. Click **Add** to add the mailing address.
6. Click **Commit**.

Related topics:

Add Address field descriptions on page 99

Modifying a mailing address

About this task

You can use this functionality to modify the mailing address of a user.

Note:

You cannot modify a shared address using this feature.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - Select a user, and click **Edit** > **Identity** > **Address**.
   - Select a user, and click **View** > **Edit** > **Identity** > **Address**.
4. Under **Address**, select the mailing address you want to modify and click **Edit**.
5. On the Edit Address page, modify the information.
6. Click **Add**.
7. Click **Commit**.

Related topics:

Edit Address field descriptions on page 101

Deleting a mailing address

About this task

You can use this functionality to delete a private mailing address from the database. If the mailing address you want to delete is a shared mailing address, the system removes the mailing address from the user's mailing address list, but not from the database.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. Perform one of the following steps:
   - If you are on the New User Profile page or on the User Profile Duplicate page and have added a mailing address, then navigate to **Identity** > **Address**.
   - On the User Management page, select a user and click **Edit** > **Identity** > **Address** .
   - On the User Management page, select a user and click **View** > **Edit** > **Identity** > **Address** .
4. Select the mailing address you want to delete and click **Delete**.
5. Click **Commit**.

Choosing a shared address

About this task

You can use this functionality to choose a shared address for a user from a set of common addresses. With this functionality, you can add, modify, and delete a shared address.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To assign shared addresses to a new user account while setting it up, click **New**.
   - To assign shared addresses to an existing user account, select a user and click **Edit**.
4. On the New User Profile page or the User Profile Edit page, click **Identity** > **Address** > **Choose Shared Address**.
5. On the Choose Address page, select one or more shared addresses.
6. Click **Select**.
7. Click **Commit**.

   When you choose a shared address for a new user, ensure that you have entered valid information in all the mandatory fields on all the tabs of the New User Profile page before you click **Commit**. If you fail to do so, the system displays an error message.

Related topics:

Choose Address field descriptions on page 102

Add Address field descriptions

Use this page to add the mailing address of the user.

Field	Description
Address Name	Displays the unique label that identifies the mailing address.
Address Type	Displays the mailing address type such as home or office address.

Field	Description
Building	Displays the name of the building.
Room	Displays the number or name of the room.
Street	Displays the name of the street.
City	Displays the name of the city or town.
State or Province	Displays the full name of the province.
Postal Code	Displays the postal code or zip code used by postal services to route mail to a destination. In the United States, this is Zip code.
Country	Displays the name of the country.

Phone Details section

Field	Description
Business Phone	Displays the business phone number of the user.
Other Business Phone	Displays the secondary or alternate business phone number, if applicable.
Home Phone	Displays the residential phone number of the user.
Other Home Phone	Displays the secondary or alternate residential phone number, if applicable.
Mobile Phone	Displays the mobile number of the user.
Other Mobile Phone	Displays the secondary or alternate mobile number of the user, if applicable.
Fax	Displays the telephone number for direct reception of faxes.
Pager	Displays the number used to make calls to the user's pager.
Other Pager	Displays the secondary or alternate number used to make calls to the user's pager.

Button	Description
Add	Adds the mailing address of the user.
Cancel	Cancels the add address operation.

Related topics:

Adding a shared address on page 416
Modifying a shared address on page 417

Edit Address field descriptions

Use this page to modify the mailing address of a user.

Field	Description
Address Name	Displays the unique label that identifies the mailing address.
Address Type	Displays the type that identifies whether mailing address is a home or office address.
Building	Displays the name of the building.
Room	Displays the number or name of the room.
Street	Displays the name of the street.
City	Displays the name of the city or town.
State or Province	Displays the full name of the province.
Postal Code	Displays the postal code or zip code used by postal services to route mail to a destination. In the United States, this is the Zip code.
Country	Displays the name of the country.

Phone Details section

Field	Description
Business Phone	Displays the business phone number of the user.
Other Business Phone	Displays the secondary or alternate business phone number, if applicable.
Home Phone	Displays the residential phone number of the user.
Other Home Phone	Displays the secondary or alternate residential phone number, if applicable.
Mobile Phone	Displays the mobile number of the user.
Other Mobile Phone	Displays the secondary or alternate mobile number of the user, if applicable.
Fax	Displays the telephone number for direct reception of faxes.
Pager	Displays the number used to make calls to the user’s pager.

Field	Description
Other Pager	Displays the secondary or alternate number used to make calls to the user's pager.

Button	Description
Done	Saves the changes that you make.
Cancel	Cancels the modify address operation.

Choose Address field descriptions

Use this page to choose a shared address for the user.

Field	Description
Name	Displays the unique label that identifies the address.
Address Type	Displays the mailing address type such as home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code used by postal services to route mail to a destination. In the United States, this is Zip code.
Province	Displays the full name of the province.
Country	Displays the name of the country.

Button	Description
Select	Adds the selected mailing address as the shared contact for the user account.
Cancel	Cancels the choose address operation.

Managing bulk import and export

Bulk import and export

In System Manager, you can bulk import and export user profiles and global settings. To import data in bulk, you must provide an XML file as input file. While exporting data in bulk, the data

is exported to an XML file. The System Manager database stores the imported user profiles and global settings data.

You can import and export the following user attributes in bulk:

- Identity Data
- Communication Profile Set
- Handles
- Communication profiles (CM Endpoint data, Messaging data, Session Manager data, CS1000 Endpoint Profile data, CallPilot Messaging Profile data, MMCS Conferencing Profile data, and B5800 Branch Gateway data)

You can import and export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- System Presence access control list (ACLs)

Important:

System Manager 6.2 does not support the bulk import and export of roles.

Key features of Bulk Import and Export

- Supports import of user profiles and global settings through XML file. Also, supports export of data to an XML file.
- Supports the following error configurations:
  - Abort on first error: Aborts import of user records when the import user operation encounters the first error in the import file containing the user records.
  - Continue processing other records: Imports the next user record even if the import user operation encounters an error while importing a user record.
- Supports the following import types:
  - A *Partial Import* type helps import of users with specific user attributes.
  - A *Complete Import* helps import of users with all user attributes.
- Provides various configuration options if a record to be imported matches an existing record in the database. You can configure to skip, replace, merge, or delete a matching record that already exists and re-import data.
- Supports scheduling of bulk import jobs from the System Manager Web console.
- Displays import job details, such as job scheduled time, job end time, job status, job completion status in percentage, number of user records in the input file, number of user records in the input file with warnings, and number of user records in the input file that failed to import. Also, provides the link to the Scheduler user interface.
- Supports cancellation and deletion of an import job.

- Maintains logs of records that fail to import and that require manual intervention.
- Supports download of failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and re-import the records into the database.

About bulk import of users

You can use the bulk import functionality to import users in bulk with their attributes from an XML file. The XML file must conform to XML schema definition. For more information, see XML Schema Definition for bulk import of users on page 130. See Sample XML for bulk import of users with all attributes on page 142 for the sample XML file for bulk import of user.

You can perform the following tasks with the bulk import functionality:

- Abort or continue the import process when the import user operation encounters first error in the user input file.
- Perform the following import types:
  - A *Partial* import type helps import of users with specific user attributes.
  - A *Complete* import type helps import of users with all user attributes.
- Skip import of the users that already exist in the database. Use this option to import new users from the XML file.
- Replace the users in the database with the new users from the file you imported. The system performs the following actions:
  - Replaces all items of user collection attributes such as CommprofileSet and Contactlist.
  - Removes the existing items.
  - Adds the new items from the XML.
  - Updates the single-value user attributes.

  For example, the user John Miller has StationA and EndpointB as existing commprofiles in default commprofileset and you import an XML file containing users with StationC and EndpointB with *Replace* option. After you import, John Miller has commprofiles StationC and EndpointB in the default commprofileset.

Note:

For CS1000 Endpoint Profile and CallPilot Messaging Profile, you cannot import both communication profile and user at the same time. You must add the user and then merge the profile.

- Update and merge the user attributes data from the imported file to the existing data. The system performs the following actions:
  - Merges items of user collection attributes such as CommprofileSet and Contactlist.
  - Retains and updates the existing items.
  - Adds the new items from the XML.
  - Updates the single-value user attributes.

  For example, the user John Miller has StationA and EndpointB as existing commprofiles in default commprofileset and you import an XML file containing users with StationC and EndpointB with *Replace* option. After you import, John Miller has commProfiles StationA, StationC, EndpointB in the default commprofileset.
- Delete the user records from the database that match the records in the input XML file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of user records in the input file
  - Total number of user records with warnings in the input file
  - Total number of user records that fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.
- Download failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and import the records again to the database.

The following two XML schema definitions are available based on the complete and partial import types:

- XML schema definition for bulk import of users: See XML Schema Definition for bulk import of users on page 130. Use this XML schema definition to add and update (Merge/Replace) users. This schema addresses complete user attributes. For a sample XML that conforms to the XML schema definition, see Sample XML for bulk import of users with minimal attributes on page 141 and Sample XML for bulk import of users with all attributes on page 142.
- XML schema definition for partial import of users: See XML Schema Definition for partial import of users on page 149. Use the XML schema definition to add and update (Merge/Replace) users. You must use this schema to import users with specific user attributes.

For a sample XML that conforms to this XML schema definition, see Sample XML for partial import of users on page 151.

To delete bulk users, a separate XML schema definition is defined. See XML Schema Definition for bulk deletion of users on page 154. For a sample XML that conforms to delete bulk users XML schema definition, see Sample XML for bulk deletion of users on page 154.

Bulk importing of users

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Users**.

   Also, to gain access to **Import users**, from the System Manager console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import users page, enter the complete path of the file in the **Select File** field.

   Also, you can click **Browse** to locate and select a file.
4. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**
5. Select **Complete** as the import type.
6. Select one of the following import options:
   - To skip users in the import file that match the existing user records in the database, click **Skip**.
   - To replace the users in the database with the new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.
   - To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
   - To delete the user records in the database that match the records in the imported file, click **Delete**.
7. To run the job, in the **Job Schedule** section, select one of the following options:
   - To import the users immediately, click **Run immediately**.
   - To import the users at a specified time, click **Schedule later**, and set date and time.
8. Click **Import**.

   If you use the default configurations option **Importing Users** > **Add Users** in the database, the system imports the next user record even if the import user operation

encounters an error while importing a user record. The system logs an error. Skip import of users that already exist in the database. The system schedules the import job to run immediately.

Note:

The operations, Communication Manager Synchronization and Bulk Import of users, must not overlap in time. If Bulk Import of users is in progress and Communication Manager Synchronization is started, the current records under process fail. After the synchronization is complete, the remaining bulk import records process successfully. You must reimport the records that fail during synchronization.

Related topics:

[About bulk import of users](#) on page 104
[List of XML Schema Definitions and sample XMLs for bulk import](#) on page 129
[Attribute details defined in Import user XSD](#) on page 228
[Attribute details defined in Delete User XSD](#) on page 238
[Attribute details defined in the CM Endpoint profile XSD](#) on page 239
[Attribute details defined in the Messaging communication profile XSD](#) on page 267
[Attribute details defined in the Session Manager communication profile XSD](#) on page 276

About bulk export of users

In System Manager, you can export users in bulk from the System Manager database using CLI. While exporting in bulk, the system exports the data to an XML file.

You can export the following user attributes in bulk:

- Identity Data
- Communication Profile Set
- Handles
- Communication profiles (CM Endpoint data, Messaging data, Session Manager data, CS1000 Endpoint Profile data, CallPilot Messaging Profile data, MMCS Conferencing Profile data, and B5800 Branch Gateway data)

Note:

For security reasons, the system does not export the password fields in the XML file.

You can export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- System Presence access control list (ACLs)

The Export User process creates an archive file containing one or more XML files. While exporting users records, if the number of exported records exceed the limit of records that an XML file can hold, the system creates multiple XML files. The system packages the XML files in a zip file.

The XML file conforms to the XML schema definition that supports import of user. This schema addresses the complete user attributes, for more information, see XML Schema Definition for bulk import of users on page 130.

The system generates the XML file on the System Manager server. You can specify the location of the file you want to export while running the Export User job.

You can schedule an export user job. The job parameter provides an option to specify the schedule time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

When you import the same file to a new system, you must provide the password for users with the *System Administrator* role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with the *System Administrator* role fails.

To import users with the *System Administrator* role, in the XML file for the users, add the following XML tag after the `<username>` tag:

```
<userPassword> provide password for user </userPassword>
```

The system imports the other user records with non system administrator roles and automatically sets the password to `Avaya123$` for **Complete Merge/Replace** import type. For **Partial Merge/Replace** import type, if you do not specify the password, the existing password remains.

System Manager Bulk export utility is available in the form of CLI utility. The utility is in the *$MGMT_HOME*`/upm/bulkexport` directory, where *MGMT_HOME* is an environment variable that represents the System Manager HOME path.

Bulk exporting of users

Before you begin

Start an SSH session.

Procedure

1. Log in to System Manager using SSH as `root`.

2. At the command prompt, change the directory to *$MGMT_HOME*/upm/bulkexport/exportutility.

   MGMT_HOME is an environment variable that represents the System Manager HOME path.

3. Type `# sh exportUpmUser.sh … [OPTIONS]`.

   The optional parameters include:

   - *-f*. The file name prefix of the file that you export.
   - *-r*. The number of records per file.
   - *-d*. The location of the file that you export.
   - *-s*. The start index of record.
   - *-e*. The number of records you export.
   - *-t*. The job scheduling time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

4. **(Optional)** To modify the optional parameters, change the `$MGMT_HOME/upm/bulkexport/exportutility/bulkexportconfig.properties` file, where *MGMT_HOME* is an environment variable that represents the System Manager HOME path.
   For example, `# sh exportUpmUsers.sh –f userExport –r 1000 –s 0 –e 1000`.

Related topics:

[About bulk export of users](#) on page 107
[List of XML Schema Definitions and sample XMLs for bulk import](#) on page 129
[Attribute details defined in Import user XSD](#) on page 228
[Attribute details defined in Delete User XSD](#) on page 238
[Attribute details defined in the CM Endpoint profile XSD](#) on page 239
[Attribute details defined in the Messaging communication profile XSD](#) on page 267
[Attribute details defined in the Session Manager communication profile XSD](#) on page 276

Configuration options for bulk import of users

You can bulk import only the selected user attributes data for one or more users existing in the database. The XML file must conform to XML schema definition, for more information, see [XML Schema Definition for partial import of users](#) on page 149. For a sample XML file for import of user, see [Sample XML for partial import of users](#) on page 151.

The following configuration options are available for import of users:

- Abort or continue the import process when the import user operation encounters first error in the user input file.
- Perform one of the following import types:
  - The partial import type. Helps import of users with specific user attributes.
  - The complete import type. Helps import of users with all user attributes.
- If a matching record already exists, you can:
  - Replace the users in the database with the new users from the file you imported. For example, you can replace the existing contact list for a user with a new contact list.
  - Merge the user attributes data from the imported file to the existing data. For example, you can add a new contact in the list of contacts for the user and update the name of the user.
  - Delete the user records from the database that match the records in the input XML file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of user records in the input file
  - Total number of user records with warnings in the input file
  - Total number of user records that fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.
- Download failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and import the records again to the database.

Bulk importing of partial user attributes for a user

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.

2. Click **Import > User Management > Users**.

   Also, to gain access to **Import users**, from the System Manager console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.

3. On the Import users page, enter the complete path of the file in the **Select File** field.

   Also, you can click **Browse** to locate and select a file.

4. Select one of the following error configuration options:

   - **Abort on first error**
   - **Continue processing other records**

5. Select **Partial** as the import type.
6. Select one of the following options to handle matching records:

   - To replace the existing attribute data of a matching user in the database with the new data from the imported file, click **Replace**.
   - To update and merge the user attributes data from the imported file to the existing data, click **Merge**.

7. To run the job, in the **Job Schedule** section, select one of the following options:

   - To import the users immediately, click **Run immediately**.
   - To import the users at a specified time, click **Schedule later**, and set date and time.

8. Click **Import**.

Related topics:

About bulk import of users on page 104
Configuration options for bulk import of users on page 109
List of XML Schema Definitions and sample XMLs for bulk import on page 129
Attribute details defined in Import user XSD on page 228
Attribute details defined in Delete User XSD on page 238
Attribute details defined in the CM Endpoint profile XSD on page 239
Attribute details defined in the Messaging communication profile XSD on page 267
Attribute details defined in the Session Manager communication profile XSD on page 276

Making exported user data compatible for partial user import

Use this section to update user attributes partially. XML file format contains the user records that System Manager exports. You must update selected user attributes in the exported XML file and then import the XML file. You require this procedure because export users generate XML file conforming to this XML Schema Definition. For more information, see XML Schema

Definition for bulk import of users on page 130. Partial import type uses a different XML schema definition, for more information, see XML Schema Definition for partial import of user attributes on page 149.

Before you begin

Export the users in bulk and generate the XML file.

About this task

For partial import of users, make the following changes in the user export XML file. You can generate the XML file by exporting users in bulk.

Procedure

1. Perform the following steps:
   a. Locate the following content in the generated XML file:

```
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:ns3="http://xml.avaya.com/schema/import1"
xmlns:ns4="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd">
```

   b. Modify `tns:users` to `tns:deltaUserList`.
   c. Remove `tns="http://xml.avaya.com/schema/import"`.
   d. Modify `ns4="http://xml.avaya.com/schema/deltaImport"` to `tns="http://xml.avaya.com/schema/deltaImport"`
   e. Modify `xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">` to `xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport userdeltaimport.xsd ">`

   After you modify the XML file as instructed in Step b through Step e, the content in Step a changes to:

```
<tns:deltaUserList xmlns:ns3="http://xml.avaya.com/schema/import1"
xmlns:tns="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
```

2. Replace all instances of:
   - `<tns:user>` with `<tns:userDelta>`
   - `</tns:user>` with `</tns:userDelta>`
   - `<tns:users>` with `<tns:deltaUserList>`
   - `</tns:users>` with `</tns:deltaUserList>`

Next steps

You can now make the updates in the XML file and import the changes to update the user attributes in the database.

About Bulk Import Encryption utility

System Manager Import User supports import of encrypted user password field and the plain text Communication Profile password field into the database. For importing a user XML file with encrypted password, System Manager provides BulkImportEncryptionUtil, a utility tool that encrypts the “userPassword” and “commPassword” fields in the user import input file.

The utility tool takes an XML file with plaintext password field values as input. This utility encrypts the password fields and generates an XML file with encrypted password field. You can use the XML file to import user.

BulkImportEncryptionUtil is a standalone Java program. You can run the utility on any machine that has Java installed on it.

Encrypt passwords in user import file using BulkImportEncryptionUtil running on Windows operating system

Before you begin

JDK 1.6 is installed on your computer. If the computer does not have JDK 1.6 installed, use the http://java.sun.com/javase/downloads/index.jsp URL to download JDK 1.6.

Procedure

1. Extract the contents of the `um_bulkimport-encryptUtil.zip` file from `$MGMT_HOME/upm/utilities` into a local folder.

   The `um_bulkimport-encryptUtil.zip` file contains the following files:

   - `um_bulkimport-encryptUtil.jar`
   - `log4j.jar` and script files
   - `um_bulkimport-encryptUtil.bat`
   - `um_bulkimport-encryptUtil.sh`
   - `Readme.txt`

2. At the command prompt, type `um_bulkimport-encryptUtil.bat <import|deltaimport> <xmlfilename> <basenamespaceprefix> <deltanamespaceprefix>`, where:

   - *import*|*deltaimport* specifies whether the input XML file has data for complete import or partial import. For complete import, this option value is `import` and for partial import this option value is `deltaimport`.
   - `xmlfilename` is the name of the XML file with complete path of the XML file that contains the data for importing the users data

- *basenamespaceprefix* is the namespace prefix in the input XML file. In the following example, `tns` is the value for the *basenamespaceprefix* parameter.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd" >
```

- *deltanamespaceprefix* is the namespace prefix given in the partial import file. Specify this parameter if you are performing a partial import. In the following example, the *deltanamespaceprefix* value is `delta` and *basenamespaceprefix* value is `tns`.

```
<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList
xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
```

Related topics:

About Bulk Import Encryption utility on page 113

Encrypt passwords in user import file using BulkImportEncryptionUtil running on Linux Operating System

Before you begin

Install JDK 1.6 on your computer. If the computer does not have JDK 1.6 installed, use the http://java.sun.com/javase/downloads/index.jsp URL to download JDK 1.6.

Procedure

1. Extract the contents of the `um_bulkimport-encryptUtil.zip` file from `$MGMT_HOME/upm/utilities` into a local folder.

   The `um_bulkimport-encryptUtil.zip` file contains the following files:

   - `um_bulkimport-encryptUtil.jar`
   - `log4j.jar` and script files
   - `um_bulkimport-encryptUtil.bat`
   - `um_bulkimport-encryptUtil.sh`
   - `Readme.txt`

2. At the command prompt, type `um_bulkimport-encryptUtil.sh <import|deltaimport> <xmlfilename> <basenamespaceprefix> <deltanamespaceprefix>`, where:

- *import* | *deltaimport* specifies whether the input XML file has data for complete import or partial import. For complete import, this option value is `import` and for partial import this option value is `deltaimport`.
- `xmlfilename` is the name of the XML file with complete path of the XML file that contains the data for importing the users data
- *basenamespaceprefix* is the namespace prefix in the input XML file. In the following example, `tns` is the value for the *basenamespaceprefix* parameter.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd" >
```

- *deltanamespaceprefix* is the namespace prefix given in the partial import file. Specify this parameter if you are performing a partial import. In the following example, the *deltanamespaceprefix* value is `delta` and *basenamespaceprefix* value is `tns`.

```
<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList
xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
```

Related topics:

About Bulk Import Encryption utility on page 113

Import user considerations

- If the comprofileset has associated handlelist/commprofilelist, you cannot update (merge/replace) commprofileset attributes (name,Isprimary) .

  To move handlelist and commprofilelist from one commprofileset to another, perform the following:

  a. Perform Replace - Import file with no commprofileset.
  b. Perform Update (merge/replace) - Import file with the new commprofileset with associated handlelist and commprofiles.

- For security reasons, you do not export the **Password** fields in the XML file.

  When you import the same file to a new system, you must provide the password for users with the *System Administrator* role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with the *System Administrator* role fails.

To import users with the *System Administrator* role, in the XML file for the users, add the following XML tag after the `<username>` tag:

```
<userPassword> provide password for user </userPassword>
```

The system imports the other user records with non System Administrator roles and automatically sets the password to `Avaya123$` for **Complete Merge/Replace** import type. For **Partial Merge/Replace** import type, if you do not specify the password, the existing password remains.

- To enhance the performance of a file with large user records, split the file into smaller file sizes. For example, you can split a user import file of 15 Kb into three files of 5 Kb each. To speed up the import process, schedule three import jobs in parallel. System Manager does have the ability to process multiple files concurrently.

Scheduling a user import job

System Manager supports scheduling of bulk import jobs from the System Manager console. You can schedule a job to run immediately or at a later time.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Users**.

   Also, to gain access to **Import users**, from the System Manager console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import users page, enter the complete path of the file in the **Select File** field.

   Also, you can click **Browse** to locate and select a file.
4. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**
5. Select one of the following import options:
   - To skip users in the import file that match the existing user records in the database, click **Skip**.
   - To replace the users in the database with the new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.
   - To update and merge the user attributes data from the imported file to the existing data, click **Merge**.

- To delete the user records in the database that match the records in the imported file, click **Delete**.

6. In the Job Schedule section:
   a. Click **Schedule later**.
      To run the user import job immediately, click **Run immediately**. When you select this option, the fields related to scheduling become unavailable.
   b. Enter the date in the **Date** field.
      You can use the calender icon to select a date.
   c. Enter the time in the **Time** field in the HH:MM:SS format.
   d. Enter the time zone in the **Time Zone** field.
7. Click **Import**.
   The page displays the scheduled job in the Manage Jobs section.

Aborting a user import job on first error

System Manager supports the following error configurations:

- Abort on first error: Aborts import of the user records when the import user operation encounters the first error in the import file containing the user records.
- Continue processing other records: Imports the next user record even if the import user operation encounters an error while importing a user record.

About this task

The user import process may encounter errors at the time of importing of users. Use this feature to configure actions when you encounter the first error. You can choose to abort the user import process or continue the import process.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Users**.
   Also, to gain access to **Import users**, from the System Manager console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import users page, enter the complete path of the file in the **Select File** field.
   Also, you can click **Browse** to locate and select a file.
4. Click **Abort on first error** to choose error configuration options.
5. Select one of the following import options:

- To skip users in the import file that match the existing user records in the database, click **Skip**.
- To replace the users in the database with the new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.
- To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
- To delete the user records in the database that match the records in the imported file, click **Delete**.

6. Choose or enter the appropriate information for remaining fields.
7. Click **Import**.

Canceling a user import job

You can cancel a job only when the job is in the PENDING EXECUTION or RUNNING state.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Users**.

   Also, to gain access to **Import users**, from the System Manager console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import Users page, select the job from the table in the Manage Jobs section.
4. Click **Cancel job**.

Deleting a user import job

System Manager supports deleting of jobs. **Delete job** option removes the job information from the database.

About this task

You can delete a job only when the status of the job is SUCCESSFUL. To interrupt a job that is running or pending, use the **Cancel job** option.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Users**.

   Also, to gain access to **Import users**, from the System Manager console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import Users page, select the job to delete from the table in the Manage Jobs section.
4. Click **Delete job**.

Viewing a user import job on the Scheduler page

You can view an import job on the Scheduler Web page. You can perform all operations on a job that Scheduler supports from the Scheduler page.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Users**.

   Also, to gain access to **Import users**, from the System Manager console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import Users page, select a job from the table in the Manage Jobs section.
4. Click the link displayed in the **Job Name** column.
   The Scheduler page displays the details of the job. You can perform operations on the job that the Scheduler supports for the job.

Viewing the details of a user import job

You can view the following details of an import job:

- Job name
- Job scheduled by
- Job scheduled start time

- Selected error configuration option
- Selected import type option
- Selected import option
- Job end time
- Job status
- Import file name
- Total number of user records in the import file
- Total number of user records successfully imported
- Total number of user records that failed to import
- Total number of warnings
- Percentage complete status

About this task

You can view the error message for each user record that fails to import. You can download the failed user records in an XML file format. You can modify the XML file and import the file again.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Users**.

   Also, to gain access to **Import users**, from the System Manager console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import Users page, select a job to view from the table in the Manage Jobs section.
4. Click **View job**.
   The Job Detail page displays the details of the selected job.

Bulk import of global user settings

You can use the *Import Global Settings* functionality to import global settings in bulk from an XML file. The XML file must conform to XML schema definition, for more information, see XML Schema Definition for bulk import of global setting records on page 213. For sample XML file for import global settings, see Sample XML for bulk import of global setting records on page 219.

You can perform the following tasks with Import Global Settings:

- Abort or continue the import process when the import operation encounters first error in the global user settings input file.
- Skip importing the global user settings records that already exist in the database. Use this option to import new global user settings records and retain the existing users.
- Update and merge the global user settings attributes data from the imported file to the existing data in the attributes.
- Replace all the global user settings records in the database with the global user settings records from the imported file.
- Delete the global setting records from the database that match the records in the input XML file.
- Schedule the bulk import job.
- View the details of an import job:
    - Job scheduled time
    - Job end time
    - Job status
    - Job completion status in percentage
    - Total number of global settings records in the input file
    - The number of global settings records with warnings in the input file
    - The number of global settings records fail to import in the input file
    - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.
- Download failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and import the records again to the database.

To add and update (Merge and Replace) global settings use XML Schema Definition for bulk import of global setting records on page 213.

To delete bulk global settings, use the XML schema definition for global settings delete, see XML Schema Definition for bulk deletion of global setting records on page 223. For a sample XML conforming to delete bulk global settings XML schema definition, see Sample XML for bulk deletion of users on page 154.

Bulk importing of global user settings records

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   Also, to gain access to **Import Global Settings**, from the System Manager console click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.
3. Click **Import** > **User Management** > **Global Settings**.
4. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

   Also, you can click **Browse** to select a file.
5. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**
6. Select one of the import options:
   - **Skip**
   - **Replace**
   - **Merge**
   - **Delete**
7. In the **Job Schedule** section, select one of the following options:
   - To run the import job immediately, click **Run immediately**.
   - To run the import job at a later time, click **Schedule later** and set the date and time.
8. Click **Import**.

Related topics:

About bulk import of users on page 104
Bulk import of global user settings on page 120
List of XML Schema Definitions and sample XMLs for bulk import on page 129

Bulk export of global user settings

In System Manager, you can export global settings in bulk from the System Manager database.

You can export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- System Presence access control list (ACLs)

The Export User process creates an archive file containing one or more XML files. While exporting the global settings records, if the number of exported records exceed the limit of records that an XML file can hold, the system creates multiple XML files. The system packages the XML files in a zip file.

The XML file conforms to the XML schema definition that supports import of global settings. This schema addresses the complete global settings attributes. For more information, see XML Schema Definition for bulk import of global setting records on page 213.

The system generates the XML file on the System Manager server. You can specify the location of the file you want to export while running the Export User job.

You can schedule an export global settings job. The job parameter provides an option to specify the schedule time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

System Manager Bulk export utility is available in the form of CLI utility. The utility is in the *$MGMT_HOME*/upm/bulkexport directory, where *MGMT_HOME* is an environment variable that represents the System Manager HOME path.

Bulk exporting of global user settings

In System Manager, you can export global settings from the System Manager database. This utility in the *$MGMT_HOME*/upm/bulkexport directory, where MGMT_HOME is an environment variable that represents the System Manager HOME path.

Before you begin

Start an SSH session.

Procedure

1. At the shell prompt, change the directory to *$MGMT_HOME*/upm/bulkexport/exportutility.

   MGMT_HOME is an environment variable that represents the System Manager HOME path.

2. Run the `# sh exportUpmGlobalsettings.sh … [OPTIONS]` command.

   The optional parameters include:

   - *-f*: The file name prefix of the file that you want to export.
   - *-r*: The number of records per file.
   - *-d*: The location of the file that you want to export.
   - *-s*: The start index of record.
   - *-e*: The number of records you want to export.
   - *-t*: The job scheduling time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.
   - *-o*: The global settings export filter, the default value is **0**.

     The following is a list of values for the global settings export filter option:

     - **0**: No Filter; **0** is considered as start index value.
     - **1**: System Default Type filter
     - **2**: Enforced users filter
     - **3**: System Rule Type filter
     - **4**: System ACL Entry Type filter
     - **5**: Shared Address filter
     - **6**: Public Contact filter

   To change the default values for the optional arguments, change the `$MGMT_HOME/upm/bulkexport/exportutility/bulkexportconfig.properties` file. *MGMT_HOME* is an environment variable that represents the System Manager HOME path.

   For example, `# sh exportUpmGlobalsettings.sh –f globalSettingExport –r 1000 –s 0 –e 1000 –o 1`.

Related topics:

[About bulk export of users](#) on page 107
[Bulk export of global user settings](#) on page 123
[List of XML Schema Definitions and sample XMLs for bulk import](#) on page 129

Scheduling a global user settings import job

About this task

System Manager supports scheduling of bulk import jobs from the System Manager console. With the scheduling utility, you can schedule an import job to run immediately or at a later time.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   Also, to gain access to **Import Global Settings**, from the System Manager console click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.
3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

   Also, you can click **Browse** to select a file.
4. Select one of the following error configuration options:

   - **Abort on first error**
   - **Continue processing other records**
5. Select one of the import options:

   - **Skip**
   - **Replace**
   - **Merge**
   - **Delete**
6. In the the **Job Schedule** section:

   a. Click **Schedule later**.

      To run the import job immediately, click **Run immediately**. After you select this option, the fields related to scheduling become unavailable.

   b. Enter the date in the **Date** field.

      You can use the calender icon to select a date.

   c. Enter time in the **Time** field in the HH:MM:SS format.

   d. From the **Time Zone** field, select a time zone.
7. Click **Import**.
   The system displays the scheduled job in the Manage Jobs section.

Viewing details of a global user settings import job

You can view the following details of an import job:

- Job name
- Job scheduled by
- Job scheduled start time
- Job end time
- Job status
- Import file name
- Total number of user records in the import file
- Total number of user records successfully imported
- Total number of user records that failed to import
- Percentage complete status

About this task

You can view the error message for each user record that fails to import. You can download the failed user records in an XML file format. You can modify the XML file and import the file again.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   Also, to gain access to **Import Global Settings**, from the System Manager console click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.
3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
4. Click **View job**.
   The Job Detail page displays the details of the selected job.

Viewing a global user settings import job on the Scheduler page

About this task

You can view and perform all operations on an import job that the scheduler supports from the Scheduler page.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   Also, to gain access to **Import Global Settings**, from the System Manager console click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.
3. On the Import Global Settings page, select a job from the table in the Manage Job section.
4. Click the link in the **Job Name** column.
   The Scheduler page displays the details of the job.

Aborting a global user settings import job on first error

System Manager supports the following error configurations:

- Abort on first error. Aborts importing of the global settings records when the import global settings operation encounters the first error in the import file that contains the global settings records.
- Continue processing other records. Imports the next global settings record even if the import operation encounters an error while importing a global settings record.

About this task

You can abort an import process when the import process encounters the first error in the input file while processing the global user settings records.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   Also, to gain access to **Import Global Settings**, from the System Manager console click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.
3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

   Also, you can click **Browse** to select a file.
4. Select **Abort on first error** as the error configuration option.
5. Select one of the import options:

   - **Skip**

- **Replace**
- **Merge**
- **Delete**

6. Choose or enter the appropriate information for the remaining fields.
7. Click **Import**.

Deleting a global user settings import job

System Manager supports deletion of an import job. The **Delete job** option removes the job information from the database. You can delete a job only when the job is in the *SUCCESSFUL* state.

To interrupt a job that is running or pending, use the **Cancel job** option.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   Also, to gain access to **Import Global Settings**, from the System Manager console click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.
3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
4. Click **Delete Job**.

Canceling a global user settings import job

You can cancel a job only when the job is in the PENDING EXECUTION or RUNNING state.

Procedure

1. On the System Manager Web Console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   Also, to gain access to **Import Global Settings**, from the System Manager console click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.

3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
4. Click **Cancel job**.

List of XML Schema Definitions and sample XMLs for bulk import

The following is the list of XML Schema Definition and sample XML snippets for bulk import of users, global setting records, elements, endpoint profiles, messaging profiles, CS 1000 and CallPilot profiles, Avaya Branch Gateway profiles, agent profiles, and Session Manager profiles:

XML Schema Definition for bulk deletion of global setting records on page 223

Sample XML for bulk deletion of global setting records on page 224

Note:

You cannot use the following characters as is in the XML file. To use the characters in the import of XML files, make the following modifications:

- Less-than character (<) as <
- Ampersand character (&) as &
- Greater-than character (>) as >
- Double-quote character (") as "
- Apostrophe or single-quote character (') as '

When you copy the XML schema from the document you must take care of the line breaks.

XML Schema Definition for bulk import of users

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ext="http://
xml.avaya.com/schema/import" xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://xml.avaya.com/schema/import" version="3.0">
    <xs:annotation>
        <xs:documentation xml:lang="en"This Schema defines schema for bulk import
and export of Users. Root Element 'Users' represent collection of user (containing
1 or more users)/xs:documentation>
    </xs:annotation>
    <xs:element name="secureStore" type="tns:xmlSecureStore"/>
    <xs:element name="user" type="tns:xmlUser"/>
    <xs:element name="users">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="secureStore" type="tns:xmlSecureStore"
minOccurs="0"/>
                <xs:element name="user" type="tns:xmlUser" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="xmlUser">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---authenticationType: This defines the type of authentication that
this user will undergo at runtime to obtain access to the system.Possible Values:
BASIC,ENTERPRISE
                ---description:A text description of the user. Human readable
description of this user instance.
                ---displayName:The localized name of a user to be used when
displaying. It will typically be the localized full name. This value may be
provisioned from the user's enterprise directory entry. If it does not exist,
synchronization rules can be used to populate it for other fields e.g. Surname,
GivenName, or LoginName.
                ---displayNameAscii:This corresponds to the Console attribute-
Endpoint Display Name.The full text name of the user represented in ASCII. It is
used to support display (e.g. endpoints) that cannot handle localized text
                ---dn:The distinguished name of the user. The DN is a sequence of
relative distinguished names (RDN) connected by commas. An RDN is an attribute with
an associated value in the form of attribute=value, normally expressed in a UTF-8
string format.The dn can be used to identify the user and may be used for
```

```
authentication subject mapping. Note the dn is changeable.
               ---isDuplicatedLoginAllowed:A boolean indicator showing whether this
user is allowed a duplicate concurrent logins.A true stipulates that the user is
allow to have duplicate logins. Default value is true.
                ---isEnabled:A boolean indicator showing whether or not the user is
active. Users with AuthenticationType=Basic will fail if this value is false.This
attribute can be used to disable access between login attempts. A running session's
login will not be revocable. Alternatively the administrator can always modify the
password to disable the user from logging in.A true stipulates this is an active
user, a false used for a disabled  user. Default value is false.
                 ---isVirtualUser:A boolean indicator showing whether or not the
record is being used for a non-human entity such as an application, service,
software agent, etc. This is to be used where the entity will behave as a user and
needs to have subset of the user profile populated. If the entity does not behave
as a user and has a different trust relationship e.g. a trust certificate it should
not be treated as a virtual user. A virtual user can represent an Avaya or external
non-human entity. This attribute is provided as a convenience to track such
accounts.A true stipulates this is a virtual users, a false is used for human users.
Default value is false.
                 ---givenName:The first name of the user.
                 ---honorific:The personal title used to address a user. This is
typically a social title and not the work title which is contained in the title
attribute. This attribute can map to "PersonalTitle".
               ---loginName:This is the unique system login name given to the user.
It can take the form of username@domain or just username.This may vary across
customers. It  can be used to help provision default user handles in the CSHandle
table.The username is an alphanumeric value that must comply with the userinfo
related portion of a URI as described in rfc2396. However, it is further restricted
as ASCII characters with only the "_" and "." special characters supported.  This
is the rfc2798 "uid" attribute.
                 ---employeeNo:Employee number of user.
                 ---department:Department of employee.
                 ---organization:Organization of employee.
                 ---middleName:The middle name of the user
              ---managerName:Text name of the user's manager. This is a free formed
field and does not require the user's manager to also be a user of the solution.
This attribute was requested to support reporting needs.
                 ---preferredGivenName:The preferred first name of the user.
                 ---preferredLanguage:The individual's preferred written or spoken
language.Values will conform to rfc4646 and the reader should refer to rfc4646 for
syntax.  This format uses the ISO standard Language (ISO-639) and region (ISO-3166)
codes In the absence of a value the client's locale should be used, if no value is
set, en-US should be defaulted.
                 ---source:Free format text field that identifies the entity that
created this user record.  The format of this field will be either a IP Address/Port
or a name representing an enterprise LDAP or Avaya.
                ---sourceUserKey:The key of the user from the source system. If the
source is an Enterprise Active Directory server, this value with be the objectGUID.
               ---status:This information is to help manage provisioning activities
such as correcting or completing the provisioning of a user instance. It can also
signify that approval is needed (PENDINGAUTHZ) before a user account is sufficiently
configured to be a valid user (PROVISIONED). Possible Values:
AUTHPENDING;PENDINGAUTHZ;PROVISIONED
                 ---suffix:The text appended to a name e.g. Jr., III.
                 ---surname:The user's last name, also called the family name.
                 ---timeZone:The preferred time zone of the user. For example:
(-12:0)International Date Line West.The application consuming this information
would need to know how to translate e.g. in Java it would be
TimeZone.getTimeZone("Europe/Moscow");In the absence of a value the local services
timezone will be used.
               ---title:The job function of a person in their organizational context.
                ---userName:This is the username portion of the loginName field. It
is an alphanumeric value that must comply with the userinfo related portion of a URI
as described in rfc2396. However, it is further restricted as ASCII characters with
only the "_" and "." special characters supported.  This is the rfc2798 "uid"
```

```
attribute.
                ---userPassword:The encrypted password for this user's account.A
null password is used when the user is authenticated by the enterprise such as with
a separate source such as the enterprise LDAP.
               ---commPassword:The encrypted subscriber or communication password
with which the user logs can use to authentication with on to any CommProfile SIP
and non SIP.  This attribute is meant to be a shared across different communication
profiles and thus different communication services.
                ---userType:This enumerates the possible primary user application
types. A User can be associated with multiple user types. Possible values are
ADMINISTRATOR;COMMUNICATION USER;AGENT;SUPERVISOR;RESIDENT EXPERT;SERVICE
TECHNICIAN;LOBBY PHONE
              ---roles:Text name of a role.This value needs to pre-exist in SMGR DB
               ---localizedNames:localized name of user.
               ---address:The address of the user.
               ---securityIdentity:The SecurityIdentity is used to hold any
additional identities for a user that can be used for authentication such as their
loginName, Kerberos account name, or their X509 certificate name.
               ---ownedContactLists:It is a collection of internal or external
contacts. ContactList is owned by a specific user and has a name that a unique name
within the context of its owner.
            ---ownedContacts:It represents a non Avaya application user (external)
contact. Contacts can be collected together along with User entities into a contact
list. Contacts can be created by an administrator or an end user.
               ---presenceUserDefault:These are personal rules that are set by
presentities to define how much presence information can be shown to watchers that
are not explicitly mentioned in an ACL. There may be one User Default rule per
presentity (User), or none.
              ---presenceUserACL:These are personal rules defined by presentities
themselves on who can monitor their presence information. There may be several
entries in the list for a given presentity, each entry corresponding to one watcher.
               ---presenceUserCLDefault:This is a personal rule that is set by
presentities to define how much presence information can be shown to watchers that
belong to the users contact list. There may be one User Contact List Default rule
per presentity (Person) or none.
               ---commProfileSet:A user will have a default commprofile set.A
commprofile set can exist without any handles or commprofiles referencing it. I.e.
you can create a commprofile set without needing to also create either a handle or
a commprofile.A commprofile set can contain multiple commprofiles, but only one of
each specific type. This is enforced by having the CommProfile uniqueness constraint
include type, commprofile_set_id.
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="authenticationType" type="xs:string"/>
            <xs:element name="description" type="xs:string" minOccurs="0"/>
            <xs:element name="displayName" type="xs:string" minOccurs="0"/>
            <xs:element name="displayNameAscii" type="xs:string" minOccurs="0"/>
            <xs:element name="dn" type="xs:string" minOccurs="0"/>
            <xs:element name="isDuplicatedLoginAllowed" type="xs:boolean"
minOccurs="0"/>
            <xs:element name="isEnabled" type="xs:boolean" minOccurs="0"/>
            <xs:element name="isVirtualUser" type="xs:boolean" minOccurs="0"/>
            <xs:element name="givenName" type="xs:string"/>
            <xs:element name="honorific" type="xs:string" minOccurs="0"/>
            <xs:element name="loginName">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:maxLength value="128"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="employeeNo" type="xs:string"
                minOccurs="0" maxOccurs="1">
            </xs:element>
```

```
            <xs:element name="department" type="xs:string" minOccurs="0"
                maxOccurs="1">
            </xs:element>
            <xs:element name="organization" type="xs:string"
                minOccurs="0" maxOccurs="1">
            </xs:element>
            <xs:element name="middleName" type="xs:string" minOccurs="0"/>
            <xs:element name="managerName" type="xs:string" minOccurs="0"/>
            <xs:element name="preferredGivenName" type="xs:string" minOccurs="0"/>
            <xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
            <xs:element name="source" type="xs:string" minOccurs="0"
                maxOccurs="1"/>
            <xs:element name="sourceUserKey" type="xs:string" minOccurs="0"
                maxOccurs="1"/>
            <xs:element name="status" type="xs:string" minOccurs="0"/>
            <xs:element name="suffix" type="xs:string" minOccurs="0"/>
            <xs:element name="surname" type="xs:string"/>
            <xs:element name="timeZone" type="xs:string" minOccurs="0"/>
            <xs:element name="title" type="xs:string" minOccurs="0"/>
            <xs:element name="userName" type="xs:string" minOccurs="0"
                maxOccurs="1"/>
            <xs:element name="userPassword" type="xs:string" minOccurs="0"/>
            <xs:element name="commPassword" type="xs:string" minOccurs="0"/>
            <xs:element name="userType" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="roles" minOccurs="0">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="role" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="localizedNames" type="tns:xmLocalizedNames"
minOccurs="0" maxOccurs="1"/xs:element>
            <xs:element name="address" type="tns:xmlAddress" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="securityIdentity" type="tns:xmlSecurityIdentity"
minOccurs="0" maxOccurs="unbounded"/>
            <!-- Contact list Entries -->
            <xs:element name="ownedContactLists" minOccurs="0">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="contactList" type="tns:xmlContactList"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="ownedContacts" minOccurs="0">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="contact" type="tns:xmlContact"
maxOccurs="unbounded"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <!-- Presence ACL User Entries -->
          <xs:element name="presenceUserDefault" type="tns:xmlPresUserDefaultType"
minOccurs="0"/>
            <xs:element name="presenceUserACL" type="tns:xmlPresUserACLEntryType"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceUserCLDefault"
type="tns:xmlPresUserCLDefaultType" minOccurs="0"/>
            <xs:element name="commProfileSet" type="tns:xmlCommProfileSetType"
minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
```

```
    </xs:complexType>
    <xs:complexType name="xmlSecurityIdentity">
        <xs:annotation>
            <xs:documentation xml:lang="en">
               ---SecurityIdentity:Represents the possible external identities that
a user may have for the purpose of authentication. The type and format of an
identity depends on the external Identity Provider and can include X.509
certificates or Kerberos user accounts
               ---identity:The unique external identity of the user. This is a free
text field and no format is enforced. The format will depend on the identity type.
Kerberos user account can take the form of:  username@domainName
e.g. jsmith@acme.org
               ---realm:The name of the security domain that this identity is valid
in.
                ---type:The text representation of the type of identity. Possible
values are: ?principalname?,?X509? and ?Kerberos?
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="identity" type="xs:string"/>
            <xs:element name="realm" type="xs:string" minOccurs="0"/>
            <xs:element name="type" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPresInfoTypeAccessType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---PresInfoTypeAccess: For the purpose of access control, presence
information is partitioned into several areas called Presence Info Types. Examples
of Presence Info Types would be "Telephony Presence", "Instant Messaging Presence",
"Calendar Presence", or "Full Presence".
             ---infoType:This defines the different classes of presence information.
                ---access:Presence access type possible values: ALLOW, BLOCK,
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="infoType" type="tns:xmlPresInfoTypeType"/>
            <xs:element name="access" type="xs:string" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPresACRuleType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---ACRuleType:This  contains rules that are similar to a User ACL
in the sense that its entries define access between individual presentities and
watchers. However this rule is managed by the administrator as opposed to
presentities themselves. Entries of Enforced User ACL can also be defined with
different priorities. Entries with higher priority will have more weight than
entries with lower priority.
               ---infotypeaccess:This is a link between acl entries, presence info
types, and access actions.
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="infoTypeAccess" type="tns:xmlPresInfoTypeAccessType"
minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPresUserDefaultType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---PresUserDefault:These are personal rules that are set by
presentities to define how much presence information can be shown to watchers that
are not explicitly mentioned in an ACL. There may be one User Default rule per
presentity (User), or none.
```

```
            </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType"/>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresUserCLDefaultType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---PresUserCLDefault:This is a personal rule that is set by
presentities to define how much presence information can be shown to watchers that
belong to the user's contact list. There may be one User Contact List Default rule
per presentity (Person) or none.
            </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType"/>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresUserACLEntryType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                   ---UserACLEntry:These are personal rules defined by presentities
themselves on who can monitor their presence information. There may be several
entries in the list for a given presentity, each entry corresponding to one watcher.
                    ---watcherLoginName: LoginName,if the watcher is a user.
                    ---watcherDisplayName:DisplayName,if the watcher is a contact.
            </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType">
                <xs:sequence>
                    <xs:choice>
                        <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
                        <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
                    </xs:choice>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresInfoTypeType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
              ---PresInfoType:Entries that define the difference classes of presence
information.
                ---label:A unique string that names this info type (e.g. "Telephony
Presence").
                ---filter:Internal definition of which part of presence information
is covered by this info type. The value of this field should be treated as opaque
string; it is maintained and used only by Presence services.
                 ---specFlags:This field is empty for regular info types, but for
special info types it contains a comma-separated list of keywords that identify
these types. In this version only "FULL" that represents full presence information
is supported.
        </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="label" type="xs:string"/>
            <xs:element name="filter" type="xs:string"/>
            <xs:element name="specFlags" type="xs:string" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <!-- Contact List entries -->
```

```
    <xs:complexType name="xmlContactList">
        <xs:annotation>
            <xs:documentation xml:lang="en">
               ---ContactList:The ContactList is a collection of personal or public
groups containing external contacts and/or Avaya users.
                ---name:The text name of the list. This in the context of the owner
must be unique.
                ---description:A free text description of this member.
                ---isPublic:Defines if the contact is public or personal. Default =
false.
                ---members:Represents the list of users or contacts that belong to
contact list
                ---contactListType:Specifies the type categorizing this list.
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="name" type="xs:string"/>
            <xs:element name="description" type="xs:string" minOccurs="0"/>
            <xs:element name="isPublic" type="xs:boolean"/>
           <xs:element name="members" type="tns:xmlContactListMember" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="contactListType" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContactListMember">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---ContactListMember:It supports many to many relationship between
user, Contact and ContactList.
                ---memberContact:This represents the name of the Contact.A
ContactListMember can either be a Contact or User
             ---speedDialContactAddress:A Contact Address added as a favorite entry
                ---memberUser:This represents the loginname of the User.A
ContactListMember can either be a Contact or User
                ---speedDialHandle:A handle added as a favorite entry
               ---isFavorite:A boolean indicator that reflects whether this contact
is a favorite entry. If true, the value of entryindex would show which position to
place this entry in any display.
                ---isSpeedDial:Each contact list member can also be flagged as a
favorite (a.k.a. speed dial)
                ---speedDialEntry:For either a presence buddy or favorite entry, a
specific communication address to use can be pointed to.
                ---isPresenceBuddy:Each contact list member can also be flagged as
a presence buddy
              ---label:A free text short word or phrase for classifying this contact
list member.
                ---altLabel:A free text short word or phrase for classifying this
contact. This is similar to label, but it is used to store alternate language
representations.
                ---description:A free text description of this
member.
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:choice>
                <xs:sequence>
                   <xs:element name="memberContact" type="xs:string" minOccurs="0"/>
                     <xs:element name="speedDialContactAddress"
type="tns:xmlContactAddress" minOccurs="0"/>
                </xs:sequence>
                <xs:sequence>
                    <xs:element name="memberUser" type="xs:string" minOccurs="0"/>
                    <xs:element name="speedDialHandle" type="tns:xmlHandle"
minOccurs="0"/>
                </xs:sequence>
```

```
            </xs:choice>
            <xs:element name="isFavorite" type="xs:boolean"/>
            <xs:element name="isSpeedDial" type="xs:boolean"/>
            <xs:element name="speedDialEntry" type="xs:int" minOccurs="0"/>
            <xs:element name="isPresenceBuddy" type="xs:boolean"/>
            <xs:element name="label" type="xs:string" minOccurs="0"/>
            <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
            <xs:element name="description" type="xs:string" minOccurs="0"/>
            <xs:element name="priorityLevel" type="xs:int" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContactAddress">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---address:A fully qualified URI for interacting with this contact.
Any addresses added to this table should contain a qualifier e.g. sip, sips, tel,
mailto. The address should be syntactically valid based on the qualifier. It must
be possible to add via the GUI and Interface. The application must do validation.
                ---altLabel:A free text description for classifying this contact.
This is similar to ContactLabel, but it is used to store alternate language
representations.
                ---contactCategory:It represents the category of this entry e.g.
Home, Office, Mobile.
                ---contactType:It represents the type of contact this entry e.g.
phone, SIP, IM, Email.
                ---label:A free text description for classifying this contact.
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="address" type="xs:string"/>
            <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
            <xs:element name="contactCategory" type="xs:string"/>
            <xs:element name="contactType" type="xs:string"/>
            <xs:element name="label" type="xs:string" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlAddress">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                    ---addressType:Specifies the role of the address. Examples:
Home, business.
                   ---name:The Name property defines the unique label by which the
address is known. Default format for user specific address should include user name
place address type.
                    ---building:The name or other designation of a structure
                  ---localityName:The name of a locality, such as a city,   county
or other geographic region.
                   ---postalCode:A code used by postal services to route mail to a
destination. In the United States this is the zip code.
                    ---room:Name or designation of a room.
                    ---stateOrProvince:The full name of a state or province.
                    ---country:A country.
                    ---street:The physical address of the object such as an address
for package delivery
                 ---postalAddress:A free formed text area for the complete physical
delivery address. It may be used in place of the specific fields in this table.
                  ---isPrivate:A boolean indicator to specify if this address could
be shared across multiple users.True is private, false is sharable. Default is false.
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="addressType" type="xs:string"/>
            <xs:element name="name" type="xs:string"/>
            <xs:element name="building" type="xs:string" minOccurs="0"/>
            <xs:element name="localityName" type="xs:string" minOccurs="0"/>
```

```
            <xs:element name="postalCode" type="xs:string" minOccurs="0"/>
            <xs:element name="room" type="xs:string" minOccurs="0"/>
            <xs:element name="stateOrProvince" type="xs:string" minOccurs="0"/>
            <xs:element name="country" type="xs:string" minOccurs="0"/>
            <xs:element name="street" type="xs:string" minOccurs="0"/>

            <!-- Additional Attribute Support LDAP -->
            <xs:element name="businessphone" type="xs:string" minOccurs="0"/>
            <xs:element name="otherbusinessphone" type="xs:string" minOccurs="0"/>
            <xs:element name="fax" type="xs:string" minOccurs="0"/>
            <xs:element name="homephone" type="xs:string" minOccurs="0"/>
            <xs:element name="otherhomephone" type="xs:string" minOccurs="0"/>
            <xs:element name="mobilephone" type="xs:string" minOccurs="0"/>
            <xs:element name="othermobilephone" type="xs:string" minOccurs="0"/>
            <xs:element name="pager" type="xs:string" minOccurs="0"/>
            <xs:element name="pager2" type="xs:string" minOccurs="0"/>
            <!-- Additional Attribute Support LDAP - End -->


            <xs:element name="postalAddress" minOccurs="0">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:maxLength value="1024"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="isPrivate" type="xs:boolean" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContact">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---Contact:An entity that represents a non Avaya application user
(external) contact. Contacts can be collected together along with User entities into
a contact list. Contacts can be created by an administrator or an end user. Contacts
have name attributes, and owner, and can be public or personal.A contact also
includes one or more contact addresses that can be used for establishing an
interaction with the contact. Contacts can be designated as being a user's presence
buddy or added as a favorite entry (i.e. speed dial).
                ---company:The organization that the contact belongs to.
                ---description:A free text field containing human readable text
providing information on this entry.
                ---displayName:The localized name of a contact to be used when
displaying. It will typically be the localized full name. This value may be
provisioned from the user's enterprise directory entry. If it does not exist,
synchronization rules can be used to populate it for other fields e.g. Surname,
GivenName, or LoginName.
                ---displayNameAscii:The full text name of the contact represented
in ASCII. It is used to support display (e.g. endpoints) that cannot handle
localized text.
                ---dn:The distinguished name of the user. The DN is a sequence of
relative distinguished names (RDN) connected by commas. An RDN is an attribute with
an associated value in the form of attribute=value, normally expressed in a UTF-8
string format.The dn can be used to uniquely identify this record. Note the dn is
changeable.
                ---givenName:The first name of the contact.
                ---initials:Initials of the contact
                ---middleName:The middle name of the contact.
                ---preferredGivenName:The nick name of the contact.
                ---preferredLanguage:The individual's preferred written or spoken
language. Values will conform to rfc4646 and the reader should refer to rfc4646 for
syntax.  This format uses the ISO standard Language (ISO-639) and region (ISO-3166)
codes In the absence of a value the client's locale should be used, if no value is
set, en-US should be defaulted.
               ---isPublic:Defines if the contact is public or personal. Default =
```

```
false.
                ---source:Free format text field that identifies the entity that
created this user record.  The format of this field will be either a IP Address/Port
or a name representing an enterprise LDAP or Avaya.
               ---sourceUserKey:The key of the user from the source system. If the
source is an Enterprise Active Directory server, this value with be the objectGUID.
                ---suffix:The text appended to a name e.g. Jr., III.
                ---surname:The user's last name, also called the family name.
                ---title:The job function of a person in their organizational
context.Examples: supervisor, manager
                ---ContactAddress:Represents a contact's address.
              ---addresses:A fully qualified URI for interacting with this contact.
Any addresses added to this table should contain a qualifier e.g. sip, sips, tel,
mailto. The address should be syntactically valid based on the qualifier. It must
be possible to add via the GUI and Interface. The application must do validation.
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="company" type="xs:string" minOccurs="0"/>
            <xs:element name="description" type="xs:string" minOccurs="0"/>
            <xs:element name="displayName" type="xs:string"/>
            <xs:element name="displayNameAscii" type="xs:string"/>
            <xs:element name="dn" type="xs:string" minOccurs="0"/>
            <xs:element name="givenName" type="xs:string"/>
            <xs:element name="initials" type="xs:string" minOccurs="0"/>
            <xs:element name="middleName" type="xs:string" minOccurs="0"/>
            <xs:element name="preferredGivenName" type="xs:string" minOccurs="0"/>
            <xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
            <xs:element name="isPublic" type="xs:boolean"/>
            <xs:element name="source" type="xs:string"/>
            <xs:element name="sourceUserKey" type="xs:string"/>
            <xs:element name="suffix" type="xs:string" minOccurs="0"/>
            <xs:element name="surname" type="xs:string"/>
            <xs:element name="title" type="xs:string" minOccurs="0"/>
            <xs:element name="ContactAddress" type="tns:xmlContactAddress"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="addresses" type="tns:xmlAddress" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlHandle">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---HandleName:This is the name given to the user to allow
communication to be established with the user. It is an alphanumeric value that must
comply with the userinfo related portion of a URI as described in rfc2396. However,
it is further restricted as ASCII characters with only the +prefix to signify this
is an E.164 handle and "_" and "." special characters supported.Note, the handle
plus domain can be used to construct a user's Address of Record.
                ---handleType:The value reflecting the type of handle this is.
Possible values are  sip,smtp,ibm,and xmpp.
                ---handleSubType:This is an additional qualify on the handle type
to help specify which private subsystem this handle belongs to.Possible values are
e164,username,msrtc,googletalk,jabber,ibmsametime,lotousnotes,msexchage.
                ---domainName:The text name of the domain.
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="handleName" type="xs:string"/>
            <xs:element name="handleType" type="xs:string"/>
            <xs:element name="handleSubType" type="xs:string"/>
            <xs:element name="domainName" type="xs:string" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlCommProfileType">
```

```
        <xs:sequence>
            <xs:element name="commProfileType" type="xs:string"/>
            <xs:element name="commProfileSubType" type="xs:string" maxOccurs="1"
minOccurs="0"/xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlCommProfileSetType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                        ---commProfileSetName:The unique name of this CommProfile.
This is used to aid in the lookup of the CommProfile
                      ---isPrimary:A boolean value indicating whether Communication
profile is primary or not.
                    </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="commProfileSetName" type="xs:string"/>
            <xs:element name="isPrimary" type="xs:boolean"/>
            <xs:element name="handleList" minOccurs="0">
                <xs:annotation>
                    <xs:documentation xml:lang="en">
                            ---handleList:List of handles
                          ---handle:A user's address of record (AOR) is represented
by a combination of a handle (userpart) and domain (domainpart).The entity that
contains the userinfo part of an address that can be used to establish an
interaction with a user. A user can have multiple handles.
                        </xs:documentation>
                </xs:annotation>
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="handle" type="tns:xmlHandle"
maxOccurs="unbounded"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="commProfileList" minOccurs="0">
                <xs:annotation>
                    <xs:documentation xml:lang="en">
                        ---commProfileList:List of communication profile
                        ---commProfile:A communication profile  is an entity that
supports communication interactions established through Avaya Communication
Services. A communication profile is used to represent a user's subscription to a
product specific communication subsystem and contains its specific configuration
needs for the user.
                    </xs:documentation>
                </xs:annotation>
                <xs:complexType>
                    <xs:sequence>
                       <xs:element name="commProfile" type="tns:xmlCommProfileType"
maxOccurs="unbounded"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="ForgeinCommProfileType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
               ---ForeignCommProfileType:A ForeignCommProfile is used to represent
a user's address information when routing to that address is controlled by a non
Avaya system or Avaya applications not using this User CIM to populate their handles
and aliases.
                ---csEncryptionKeyId:The service will be responsible for using this
key and the secure store library API when encrypting and decrypting the password
field when respectively set or accessed by an authorized client.
```

```
                ---servicePassword:.Password is an optional field if an Avaya
application needs to authenticate with the foreign service. This field will be
stored using a reversible encryption algorithm. The key will be specified through a
reference to EncryptionKey.
            </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="ext:xmlCommProfileType">
                <xs:sequence>
                 <xs:element name="csEncryptionKeyId" type="xs:long" minOccurs="0"/>
                 <xs:element name="servicePassword" type="xs:string" minOccurs="0"/>
                    <xs:element name="serviceData" type="xs:string" minOccurs="0"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlSecureStore">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---SecureStore:The Entity is used to persist the secure store. Each
application can have a single secure store and the application name used to
represent the secure store must be unique.
                ---passwordEncrypted :This section gets generated by the encryption
util which encrypts the userPassword and CommPassword.
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="secureStoreData" type="xs:base64Binary"/>
            <xs:element name="passwordEncrypted" type="xs:boolean"/>
        </xs:sequence>
    </xs:complexType>


    <xs:complexType name="xmlLocalizedName">
        <xs:sequence>
            <xs:element name="locale" type="xs:string" minOccurs="1"
                maxOccurs="1">
            </xs:element>
            <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/
xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmLocalizedNames">
        <xs:sequence>
            <xs:element name="localizedName" type="tns:xmlLocalizedName"
minOccurs="0" maxOccurs="7"/xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

Sample XML for bulk import of users with minimal attributes

```
<?xml version="1.0" encoding="UTF-8"?>
    <!--  Root Element 'Users' represent collection of  user (containing 1 or more
users)-->
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"  xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/
schema/import userimport.xsd" >

  <tns:user>
    <authenticationType>Basic</authenticationType>
    <givenName>John</givenName>
    <loginName>jmiller@avaya.com</loginName>
    <surname>Miller</surname>
```

```
    <userPassword>mypassword</userPassword>
  </tns:user>

</tns:users>
```

Sample XML for bulk import of users with all attributes

```
<?xml version="1.0" encoding="UTF-8"?>
    <!--  Root Element 'Users' represent collection of  user (containing 1 or more
users)-->
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"  xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/
schema/import userimport.xsd">
  <!--    authenticationType: This defines the type of authentication that this user
will undergo at runtime to obtain access to the system.Possible Values:
BASIC,ENTERPRISE
    description:A text description of the user. Human readable description of this
user instance.
    displayName:The localized name of a user to be used when displaying. It will
typically be the localized full name. This value may be provisioned from the users
enterprise directory entry. If it does not exist, synchronization rules can be used
to populate it for other fields e.g. Surname, GivenName, or LoginName.
    displayNameAscii:This corresponds to the Console attribute-Endpoint Display
Name.The full text name of the user represented in ASCII. It is used to support
display (e.g. endpoints) that cannot handle localized text
    dn:The distinguished name of the user. The DN is a sequence of relative
distinguished names (RDN) connected by commas. An RDN is an attribute with an
associated value in the form of attribute=value, normally expressed in a UTF-8
string format.The dn can be used to identify the user and may be used for
authentication subject mapping. Note the dn is changeable.
    isDuplicatedLoginAllowed:A boolean indicator showing whether this user is
allowed a duplicate concurrent logins.A true stipulates that the user is allow to
have duplicate logins. Default value is true.
    isEnabled:A boolean indicator showing whether or not the user is active. Users
with AuthenticationType equals Basic will fail if this value is false.This attribute
can be used to disable access between login attempts. A running sessions login will
not be revocable. Alternatively the administrator can always modify the password to
disable the user from logging in.A true stipulates this is an active user, a false
used for a disabled  user. Default value is false.
    isVirtualUser:A boolean indicator showing whether or not the record is being
used for a non-human entity such as an application, service, software agent, etc.
This is to be used where the entity will behave as a user and needs to have subset
of the user profile populated. If the entity does not behave as a user and has a
different trust relationship e.g. a trust certificate it should not be treated as a
virtual user. A virtual user can represent an Avaya or external non-human entity.
This attribute is provided as a convenience to track such accounts.A true stipulates
this is a virtual users, a false is used for human users. Default value is false.
    givenName:The first name of the user.
    honorific:The personal title used to address a user. This is typically a social
title and not the work title which is contained in the title attribute. This
attribute can map to PersonalTitle.
    loginName:This is the unique system login name given to the user. It can take
the form of username@domain or just username.This may vary across customers. It  can
be used to help provision default user handles in the CSHandle table.The username
is an alphanumeric value that must comply with the userinfo related portion of a URI
as described in rfc2396. However, it is further restricted as ASCII characters with
only the _ and . special characters supported.  This is the rfc2798 uid attribute.
    employeeNo:Employee number of user.
    department:Department of employee.
    organization:Organization of employee.
    middleName:The middle name of the user
    managerName:Text name of the users manager. This is a free formed field and does
not require the users manager to also be a user of the solution. This attribute was
requested to support reporting needs.
    preferredGivenName:The preferred first name of the user.
```

```
    preferredLanguage:The individuals preferred written or spoken language.Values
will conform to rfc4646 and the reader should refer to rfc4646 for syntax.This
format uses the ISO standard Language ISO639 and region ISO3166 codes In the absence
of a value the clients locale should be used, if no value is set, en-US should be
defaulted.
    source:Free format text field that identifies the entity that created this user
record.  The format of this field will be either a IP Address/Port or a name
representing an enterprise LDAP or Avaya.
    sourceUserKey:The key of the user from the source system. If the source is an
Enterprise Active Directory server, this value with be the objectGUID.
    status:This information is to help manage provisioning activities such as
correcting or completing the provisioning of a user instance. It can also signify
that approval is needed (PENDINGAUTHZ) before a user account is sufficiently
configured to be a valid user (PROVISIONED). Possible Values:
AUTHPENDING;PENDINGAUTHZ;PROVISIONED
    suffix:The text appended to a name e.g. Jr., III.
    surname:The users last name, also called the family name.
   timeZone:The preferred time zone of the user. For example:  (-12:0)International
Date Line West.
    title:The job function of a person in their organizational context.
    userName:This is the username portion of the loginName field. It is an
alphanumeric value that must comply with the userinfo related portion of a URI as
described in rfc2396. However, it is further restricted as ASCII characters with
only the _ and . special characters supported.  This is the rfc2798 uid attribute.
    userPassword:The encrypted password for this users account.A null password is
used when the user is authenticated by the enterprise such as with a separate source
such as the enterprise LDAP.
    commPassword:The encrypted subscriber or communication password with which the
user logs can use to authentication with on to any CommProfile SIP and non SIP.
This attribute is meant to be a shared across different communication profiles and
thus different communication services.
   userType:This enumerates the possible primary user application types. A User can
be associated with multiple user types. Possible values are
ADMINISTRATOR;COMMUNICATION USER;AGENT;SUPERVISOR;RESIDENT EXPERT;SERVICE
TECHNICIAN;LOBBY PHONE
    roles:Text name of a role.This value needs to pre-exist in SMGR DB
    localizedNames:localized name of user.
    address:The address of the user.
    securityIdentity:The SecurityIdentity is used to hold any additional identities
for a user that can be used for authentication such as their loginName, Kerberos
account name, or their X509 certificate name.
    ownedContactLists:It is a collection of internal or external contacts.
ContactList is owned by a specific user and has a name that a unique name within the
context of its owner.
    ownedContacts:It represents a non Avaya application user (external) contact.
Contacts can be collected together along with User entities into a contact list.
Contacts can be created by an administrator or an end user.
    presenceUserDefault:These are personal rules that are set by presentities to
define how much presence information can be shown to watchers that are not
explicitly mentioned in an ACL. There may be one User Default rule per presentity
(User), or none.
    presenceUserACL:These are personal rules defined by presentities themselves on
who can monitor their presence information. There may be several entries in the list
for a given presentity, each entry corresponding to one watcher.
    presenceUserCLDefault:This is a personal rule that is set by presentities to
define how much presence information can be shown to watchers that belong to the
userss contact list. There may be one User Contact List Default rule per presentity
(Person) or none.
    commProfileSet:A user will have a default commprofile set.A commprofile set can
exist without any handles or commprofiles referencing it. I.e. you can create a
commprofile set without needing to also create either a handle or a commprofile.A
commprofile set can contain multiple commprofiles, but only one of each specific
type. This is enforced by having the CSCommProfile uniqueness constraint include
type, cs_commprofile_set_id.
-- >
```

```
  <tns:user>
    <authenticationType>BASIC</authenticationType>
    <description>this is <description/description>
    <displayName> John Miller</displayName>
    <displayNameAscii></displayNameAscii>
    <dn>dc=acme,dc=org</dn>
    <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
    <isEnabled>true</isEnabled>
    <isVirtualUser>false</isVirtualUser>
    <givenName>John</givenName>
    <honorific>Mr</honorific>
    <loginName>jmiller@avaya.com</loginName>
    <employeeNo>20060441</employeeNo>
    <department>UC</department>
    <organization>GCS</organization>
    <middleName></middleName>
    <managerName>Jay Smith</managerName>
    <preferredGivenName>John</preferredGivenName>
    <preferredLanguage>English</preferredLanguage>
    <source>LDAP</source>
    <sourceUserKey>18966</sourceUserKey>
    <status>AUTHPENDING</status>
    <suffix>Mr</suffix>
    <surname>Miller</surname>
    <timeZone>(-12:0)International Date Line West</timeZone>
    <title>Mr</title>
    <userName>jmiller</userName>
    <userPassword>password</userPassword>
    <commPassword>mycommPassword</commPassword>
    <userType>ADMINISTRATOR</userType>
    <roles>
      <role>End-User</role>
    </roles>
    <localizedNames>
    <localizedName>
    <locale>English</locale>
    <name>John</name>
    </localizedName>
    </localizedNames>
    <!--addressType:Specifies the role of the address. Examples:  Home, business.
    name:The Name property defines the unique label by which the address is known.
Default format for user specific address should include user name place address type.
    building:The name or other designation of a structure
    localityName:The name of a locality, such as a city,    county or other
geographic region.
   postalCode:A code used by postal services to route mail to a destination. In the
United States this is the zip code.
    room:Name or designation of a room.
    stateOrProvince:The full name of a state or province.
    country:A country.
   street:The physical address of the object such as an address for package delivery
    postalAddress:A free formed text area for the complete physical delivery
address. It may be used in place of the specific fields in this table.
    isPrivate:A boolean indicator to specify if this address could be shared across
multiple users.True is private, false is sharable. Default is false.
-->
     <address>
      <addressType>OFFICE</addressType>
      <name>Avaya Office</name>
      <building>building 11</building>
      <localityName>Magarpatta</localityName>
      <postalCode>411028</postalCode>
      <room>room 502</room>
      <stateOrProvince>Maharashtra</stateOrProvince>
      <country>India</country>
```

```
      <street>street</street>
      <postalAddress></postalAddress>
      <isPrivate>true</isPrivate>
    </address>
    <!--    SecurityIdentity:Represents the possible external identities that a user
may have for the purpose of authentication. The type and format of an identity
depends on the external Identity Provider and can include X.509 certificates or
Kerberos user accounts
    identity:The unique external identity of the user. This is a free text field and
no format is enforced. The format will depend on the identity type. Kerberos user
account can take the form of:  username@domainName
e.g. jsmith@acme.org
    realm:The name of the security domain that this identity is valid in.
    type:The text representation of the type of identity. Possible values are:
principalname,X509 and Kerberos
-->
    <securityIdentity>
      <identity>jmiller@acme.org </identity>
      <realm>acme</realm>
      <type>principalname</type>
    </securityIdentity>
    <!--ContactList:The ContactList is a collection of personal or public groups
containing external contacts and/or Avaya users.
    name:The text name of the list. This in the context of the owner must be unique.
    description:A free text description of this member.
    isPublic:Defines if the contact is public or personal. Default = false.
    members:Represents the list of users or contacts that belong to contact list
    contactListType:Specifies the type categorizing this list.
-->
    <ownedContactLists>
      <contactList>
        <name>MycontactList</name>
        <description>This is my contactList</description>
        <isPublic>false</isPublic>
        <!--
                memberContact:This represents the name of the Contact.A
ContactListMember can either be a Contact o  User
               speedDialContactAddress:A Contact Address added as a favorite entry
                memberUser:This represents the loginname of the User.A
ContactListMember can either be a Contact or User
                speedDialHandle:A handle added as a favorite entry
                isFavorite:A boolean indicator that reflects whether this contact
is a favorite entry. If true, the value of entryindex would show which position to
place this entry in any display.
             isSpeedDial:Each contact list member can also be flagged as a favorite
(a.k.a. speed dial)
                speedDialEntry:For either a presence buddy or favorite entry, a
specific communication address to use can be pointed to.
                isPresenceBuddy:Each contact list member can also be flagged as a
presence buddy
               label:A free text short word or phrase for classifying this contact
list member.
                altLabel:A free text short word or phrase for classifying this
contact. This is similar to label, but it is used to store alternate language
representations.
                description:A free text description of this member.
-->
    <members>
          <memberContact>Phil Bath</memberContact>
          <speedDialContactAddress>
                <address>+44-1234568</address>
                <altLabel>Phone</altLabel>
                <contactCategory>OFFICE</contactCategory>
                <contactType>PHONE</contactType>
                <label>Phone</label>
```

```
          </speedDialContactAddress.
          <isFavorite>true</isFavorite>
          <isSpeedDial>true</isSpeedDial>
          <speedDialEntry>1234</speedDialEntry>
          <isPresence>Buddytrue</isPresenceBuddy>
          <label>My Contact in Dublin office</label>
          <altLabel>Phone Number for contacting Denver office</altLabel>
          <description>Contact Details</description>
          <priorityLevel>0</priorityLevel>
        </members>
        <contactListType>CONTACTCENTER</contactListType>
      </contactList>
    </ownedContactLists>
   <!--   Contact:An entity that represents a non Avaya application user (external)
contact. Contacts can be collected together along with User entities into a contact
list. Contacts can be created by an administrator or an end user. Contacts have name
attributes, and owner, and can be public or personal.A contact also includes one or
more contact addresses that can be used for establishing an interaction with the
contact. Contacts can be designated as being a users presence buddy or added as a
favorite entry (i.e. speed dial).
    company:The organization that the contact belongs to.
    description:A free text field containing human readable text providing
information on this entry.
    displayName:The localized name of a contact to be used when displaying. It will
typically be the localized full name. This value may be provisioned from the users
enterprise directory entry. If it does not exist, synchronization rules can be used
to populate it for other fields e.g. Surname, GivenName, or LoginName.
    displayNameAscii:The full text name of the contact represented in ASCII. It is
used to support display (e.g. endpoints) that cannot handle localized text.
    dn:The distinguished name of the user. The DN is a sequence of relative
distinguished names (RDN) connected by commas. An RDN is an attribute with an
associated value in the form of attribute=value, normally expressed in a UTF-8
string format.The dn can be used to uniquely identify this record. Note the dn is
changeable.
    givenName:The first name of the contact.
    initials:Initials of the contact
    middleName:The middle name of the contact.
    preferredGivenName:The nick name of the contact.
    preferredLanguage:The individuals preferred written or spoken language. Values
will conform to rfc4646 and the reader should refer to rfc4646 for syntax. This
format uses the ISO standard Language ISO639 and region ISO3166 codes In the absence
of a value the clients locale should be used, if no value is set, en-US should be
defaulted.
    isPublic:Defines if the contact is public or personal. Default = false.
    source:Free format text field that identifies the entity that created this user
record.  The format o  this field will be either a IP Address/Port or a name
representing an enterprise LDAP or Avaya.
    sourceUserKey:The key of the user from the source system. If the source is an
Enterprise Active Directory server, this value with be the objectGUID.
    suffix:The text appended to a name e.g. Jr., III.
    surname:The users last name, also called the family name.
    title:The job function of a person in their organizational context.Examples:
supervisor, manager
    ContactAddress:Represents a contacts address.
   addresses:A fully qualified URI for interacting with this contact. Any addresses
added to this table should contain a qualifier e.g. sip, sips, tel, mailto. The
address should be syntactically valid based on the qualifier. It must be possible
to add via the GUI and Interface. The application must do validation.

-->
    <ownedContacts>
      <contact>
          <company>ABC</company>
          <description>Company ABC description</description>
          <displayName>Phil Bath</displayName>
```

```
          <displayNameAscii></displayNameAscii>
          <dn>dc=acme,dc=org</dn>
          <givenName>John</givenName>
          <initials>Mr</initials>
          <middleName>M</middleName>
          <preferredGivenName>Phil</preferredGivenName>
          <preferredLanguage>English</preferredLanguage>
          <isPublic>false</isPublic>
          <source>ldap</source>
          <sourceUserKey>123546</sourceUserKey>
          <suffix>Jr.</suffix>
          <surname>Bath</surname>
          <title>Manager</title>
      <!--
        type:The value reflecting the type of handle this is. Possible values are
username, e164, and privatesubsystem
        category:The value representing a further qualification to the contact
address. Possible values inlcude Office, Home, Mobile.
        handle:This is the name given to the user to allow communication to be
established with the user. It is an alphanumeric value that must comply with the
userinfo related portion of a URI as described in rfc2396. However, it is further
restricted as ASCII characters with only the + prefix to signify this is an E.164
handle and _ and . special characters supported.The handle and type together are
unique within a specific domain. Note, the handle plus domain can be used to
construct a users Address of Record.
        label:A free text description for classifying this contact.
        altLabel:A free text description for classifying this contact. This is
similar to ContactLabel, but it is used to store alternate language representations.
        -->
      <ContactAddress>
            <address>+44-1234568</address>
            <altLabel>Phone</altLabel>
                <contactCategory>OFFICE</contactCategory>
                <contactType>PHONE</contactType>
                <label>Phone</label>
      </ContactAddress>
      <addresses>
      <!--
       addressType:The unique text name of the address type. Possible values are:
Home, business.
        name: The Name property defines the unique label by which the address is
known. Default format for user specific address should include user name place
address type.
        building:The name or other designation of a structure.
        localityName:The name of a locality, such as a city, county or other
geographic region.
        postalCode:A code used by postal services to route mail to a destination.
In the United States this is the zip code.
        room:Name or designation of a room.
        stateOrProvince:The full name of a state or province.
        country:A country.
        street:The physical address of the object such as an address for package
delivery
        postalAddress:A free formed text area for the complete physical delivery
address. It may be used in place of the specific fields in this table.
-->

          <addressType>office</addressType>
          <name>Phil Bath</name>
          <building>building A</building>
          <localityName>Magarpatta</localityName>
          <postalCode>411048</postalCode>
          <room>room 123</room>
          <stateOrProvince>MH</stateOrProvince>
          <country>India</country>
```

```
          <street>Hadapsar</street>
          <isPrivate>true</isPrivate>

      </addresses>
      </contact>
    </ownedContacts>
    <!--       PresUserDefault:These are personal rules that are set by presentities
to define how much presence information can be shown to watchers that are not
explicitly mentioned in an ACL. There may be one User Default rule per presentity
(User), or none.presentity (User), or none.
presentity (User), or none.
        label:A unique string that names this info type (e.g. Telephony Presence).
       filter:Internal definition of which part of presence information is covered
by this info type. The value of this field should be treated as opaque string; it
is maintained and used only by Presence services.
        specFlags:This field is empty for regular info types, but for special info
types it contains a comma separated list of keywords that identify these types. In
this version only FULL that represents full presence information is supported.
-->
    <presenceUserDefault>
      <infoTypeAccess>
        <infoType>
          <label>Telephony Presence</label>
          <filter>filter</filter>
          <specFlags>FULL</specFlags>
        </infoType>
        <access>BLOCK</access>
      </infoTypeAccess>
    </presenceUserDefault>
    <!--UserACLEntry:These are personal rules defined by presentities themselves on
who can monitor their presence information. There may be several entries in the list
for a given presentity, each entry corresponding to one watcher.
        label:A unique string that names this info type (e.g. Telephony Presence).
       filter:Internal definition of which part of presence information is covered
by this info type. The value of this field should be treated as opaque string; it
is maintained and used only by Presence services.
        specFlags:This field is empty for regular info types, but for special info
types it contains a comma separated list of keywords that identify these types. In
this version only FULL that represents full presence information is supported.
-->
    <presenceUserACL>
      <infoTypeAccess>
        <infoType>
          <label>ALL</label>
          <filter>filter</filter>
          <specFlags>FULL</specFlags>
        </infoType>
        <access>BLOCK</access>
      </infoTypeAccess>
      <watcherLoginName>admin</watcherLoginName>
    </presenceUserACL>
    <!--PresUserCLDefault:This is a personal rule that is set by presentities to
define how much presence information can be shown to watchers that belong to the
users contact list. There may be one User Contact List Default rule per presentity
(Person) or none.
-->
    <presenceUserCLDefault>
      <infoTypeAccess>
        <infoType>
          <label>Telephony</label>
          <filter>filter</filter>
          <specFlags>FULL</specFlags>
        </infoType>
        <access>BLOCK</access>
      </infoTypeAccess>
```

```
    </presenceUserCLDefault>
<!--commProfileSet:A user will have a default commprofile set.A commprofile set can
exist without any handles or commprofiles referencing it. I.e. you can create a
commprofile set without needing to also create either a handle or a commprofile.A
commprofile set can contain multiple commprofiles, but only one of each specific
type. This is enforced by having the CommProfile uniqueness constraint include type,
commprofile_set_id.
    HandleName:This is the name given to the user to allow communication to be
established with the user. It is an alphanumeric value that must comply with the
userinfo related portion of a URI as described in rfc2396. However, it is further
restricted as ASCII characters with only the + prefix to signify this is an E.164
handle and _ and . special characters supported.Note, the handle plus domain can be
used to construct a users Address of Record.
   handleType:The value reflecting the type of handle this is. Possible values are
sip,smtp,ibm,and xmpp.
    handleSubType:This is an additional qualify on the handle type to help specify
which private subsystem this handle belongs to.Possible values are
e164,username,msrtc,googletalk,jabber,ibmsametime,lotousnotes,msexchageo.
    domainName:The text name of the domain.
-->
   <commProfileSet>
      <commProfileSetName>Primary</commProfileSetName>
      <isPrimary>true</isPrimary>
      <handleList>
     <handle>
          <handleName>sip:abc@yahoo.com</handleName>
          <handleType>sip</handleType>
          <handleSubType>msrtc</handleSubType>
        </handle>
      </handleList>
      <!--The below is extended communication profile-->
<!--
      <commProfileList>
         <commProfile xsi:type="ext:ASMCommProfile" xmlns:ext="http://xml.avaya.com/
schema/import1">
          <commProfileType>ASM</commProfileType>
          <ext:forkingPolicy>Sequential</ext:forkingPolicy>
          <ext:origApplicationSet>Default Denever Origination</
ext:origApplicationSet>
          <ext:termApplicationSet>Default Denever Termination</
ext:termApplicationSet>
          <ext:userCommunity>Denever</ext:userCommunity>
           <ext:subscriptionSet>subscriptionSet</ext:subscriptionSet>
         </commProfile>
      </commProfileList>
--
    </commProfileSet>

  </tns:user>
</tns:users>
```

XML Schema Definition for partial import of users

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<xs:schema xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:base="http://xml.avaya.com/schema/import" xmlns:xs="http://www.w3.org/2001/
XMLSchema" targetNamespace="http://xml.avaya.com/schema/deltaImport" version="1.0">

    <xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>


    <xs:element name="userDelta" type="delta:xmlUserDelta"/>
    <xs:element name="deltaUserList" type="delta:xmlDeltaUserList"/>
```

```
    <xs:complexType name="xmlDeltaUserList">
        <xs:sequence>
            <xs:element name="secureStore" type="base:xmlSecureStore"></xs:element>
            <xs:element name="userDelta" type="delta:xmlUserDelta" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlUserDelta">
        <xs:sequence>
            <xs:element name="authenticationType"
                type="xs:string" minOccurs="0" maxOccurs="1" />
            <xs:element name="description" type="xs:string"
                minOccurs="0" />
            <xs:element name="displayName" type="xs:string"
                minOccurs="0" />
            <xs:element name="displayNameAscii" type="xs:string"
                minOccurs="0" />
            <xs:element name="dn" type="xs:string" minOccurs="0" />
            <xs:element name="isDuplicatedLoginAllowed"
                type="xs:boolean" minOccurs="0" />
            <xs:element name="isEnabled" type="xs:boolean" minOccurs="0"
                maxOccurs="1" />
            <xs:element name="isVirtualUser" type="xs:boolean"
                minOccurs="0" />
            <xs:element name="givenName" type="xs:string" maxOccurs="1"
                minOccurs="0" />
            <xs:element name="honorific" type="xs:string" minOccurs="0" />
            <xs:element name="loginName" type="xs:string" maxOccurs="1"
                minOccurs="1" />
            <xs:element name="middleName" type="xs:string"
                minOccurs="0" />
            <xs:element name="managerName" type="xs:string"
                minOccurs="0" />
            <xs:element name="preferredGivenName" type="xs:string"
                minOccurs="0" />
            <xs:element name="preferredLanguage" type="xs:string"
                minOccurs="0" />
            <xs:element name="source" type="xs:string" minOccurs="0"
                maxOccurs="1" />
            <xs:element name="sourceUserKey" type="xs:string"
                minOccurs="0" maxOccurs="1" />
            <xs:element name="status" type="xs:string"
                minOccurs="0" />
            <xs:element name="suffix" type="xs:string" minOccurs="0" />
            <xs:element name="surname" type="xs:string" minOccurs="0"
                maxOccurs="1" />
            <xs:element name="timeZone" type="xs:string" minOccurs="0" />
            <xs:element name="title" type="xs:string" minOccurs="0" />
            <xs:element name="userName" type="xs:string" maxOccurs="1"
                minOccurs="0" />
            <xs:element name="userPassword" type="xs:string"
                minOccurs="0" />
            <xs:element name="commPassword" type="xs:string"
                minOccurs="0" />
            <xs:element name="userType" type="xs:string"
                minOccurs="0" maxOccurs="unbounded" />
            <xs:element name="roles" minOccurs="0">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="role" type="xs:string"
                            minOccurs="0" maxOccurs="unbounded" />
                    </xs:sequence>
                </xs:complexType>
```

```
            </xs:element>
            <xs:element name="address" type="base:xmlAddress"
                minOccurs="0" maxOccurs="unbounded" />
            <xs:element name="securityIdentity"
              type="base:xmlSecurityIdentity" minOccurs="0" maxOccurs="unbounded" />
            <!-- Contact list Entries -->
            <xs:element name="ownedContactLists" minOccurs="0"
                maxOccurs="1">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="contactList"
                            type="base:xmlContactList" maxOccurs="1" />
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="ownedContacts" minOccurs="0">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="contact" type="base:xmlContact"
                            maxOccurs="unbounded" />
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <!-- Presence ACL User Entries -->
            <xs:element name="presenceUserDefault"
                type="base:xmlPresUserDefaultType" minOccurs="0" />
            <xs:element name="presenceUserACL"
                type="base:xmlPresUserACLEntryType" minOccurs="0"
                maxOccurs="unbounded" />
            <xs:element name="presenceUserCLDefault"
                type="base:xmlPresUserCLDefaultType" minOccurs="0" maxOccurs="1" />
            <xs:element name="commProfileSet"
              type="base:xmlCommProfileSetType" maxOccurs="unbounded" minOccurs="0">
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

Sample XML for partial import of users

```
<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
  <delta:userDelta>
    <authenticationType>ENTERPRISE</authenticationType>
    <description>this is description</description>
    <displayName>John Miller</displayName>
    <displayNameAscii></displayNameAscii>
    <dn>dc=acme,dc=org</dn>
    <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
    <isEnabled>true</isEnabled>
    <isVirtualUser>true</isVirtualUser>
    <givenName>John</givenName>
    <honorific>Mr</honorific>
    <loginName>jmiller@avaya.com</loginName>
    <middleName></middleName>
    <managerName>Jay Smith</managerName>
    <preferredGivenName>John</preferredGivenName>
    <preferredLanguage>English</preferredLanguage>
    <source>LDAP</source>
    <sourceUserKey>18966</sourceUserKey>
    <status>AUTHPENDING</status>
    <suffix>Mr</suffix>
```

```
    <surname>Miller</surname>
    <timeZone>(-12:00) International Date Line West</timeZone>
    <title>Mr</title>
    <userName>jmiller</userName>
    <commPassword>mycommPassword</commPassword>
    <userType>ADMINISTRATOR</userType>
    <roles>
      <role>End-User</role>
    </roles>
    <address>
      <addressType>OFFICE</addressType>
      <name>Avaya Office</name>
      <building>building 11</building>
      <localityName>Magarpatta</localityName>
      <postalCode>411028</postalCode>
      <room>room 502</room>
      <stateOrProvince>Maharashtra</stateOrProvince>
      <country>India</country>
      <street>street</street>
      <postalAddress></postalAddress>
      <isPrivate>true</isPrivate>
    </address>
    <securityIdentity>
      <identity>jmiller@acme.org </identity>
      <realm>acme</realm>
      <type>principalname</type>
    </securityIdentity>
    <ownedContactLists>
      <contactList>
         <name>MycontactList</name>
        <description>This is my contactList</description>
        <isPublic>false</isPublic>
        <members>
          <memberContact>Phil Bath</memberContact>
          <speedDialContactAddress>
        <address>+44-1234568</address>
        <altLabel>Phone</altLabel>
        <contactCategory>OFFICE</contactCategory>
        <contactType>PHONE</contactType>
        <label>Phone</label>
          </speedDialContactAddress>
          <isFavorite>true</isFavorite>
          <isSpeedDial>true</isSpeedDial>
        <speedDialEntry>1234</speedDialEntry>
          <isPresenceBuddy>true</isPresenceBuddy>
          <label>My Contact in Dublin office</label>
          <altLabel>Phone Number for contacting Denver office</altLabel>
          <description>Contact Details</description>
          <priorityLevel>0</priorityLevel>
        </members>
        <contactListType>CONTACTCENTER</contactListType>
      </contactList>
    </ownedContactLists>
    <ownedContacts>
      <contact>
        <company>ABC</company>
        <description>Company ABC description</description>
        <displayName>Phil Bath</displayName>
        <displayNameAscii></displayNameAscii>
        <dn>dc=acme,dc=org</dn>
        <givenName>John</givenName>
        <initials>Mr</initials>
        <middleName>M</middleName>
        <preferredGivenName>Phil</preferredGivenName>
        <preferredLanguage>English</preferredLanguage>
```

```
        <isPublic>false</isPublic>
        <source>ldap</source>
        <sourceUserKey>123546</sourceUserKey>
        <suffix>Jr.</suffix>
        <surname>Bath</surname>
        <title>Manager</title>
        <ContactAddress>
            <address>+44-1234568</address>
        <altLabel>Phone</altLabel>
        <contactCategory>OFFICE</contactCategory>
        <contactType>PHONE</contactType>
        <label>Phone</label>
        </ContactAddress>
        <addresses>
          <addressType>office</addressType>
          <name>Phil Bath</name>
          <building>building A</building>
          <localityName>Magarpatta</localityName>
          <postalCode>411048</postalCode>
          <room>room 123</room>
          <stateOrProvince>MH</stateOrProvince>
          <country>India</country>
          <street>Hadapsar</street>
          <isPrivate>true</isPrivate>
        </addresses>
      </contact>
    </ownedContacts>
    <presenceUserDefault>
      <infoTypeAccess>
        <infoType>
          <label>Telephony Presence</label>
          <filter>filter</filter>
          <specFlags>FULL</specFlags>
        </infoType>
        <access>BLOCK</access>
      </infoTypeAccess>
    </presenceUserDefault>
    <presenceUserACL>
      <infoTypeAccess>
        <infoType>
          <label>ALL</label>
          <filter>filter</filter>
          <specFlags>FULL</specFlags>
        </infoType>
        <access>BLOCK</access>
      </infoTypeAccess>
      <watcherLoginName>admin</watcherLoginName>
    </presenceUserACL>
    <presenceUserCLDefault>
      <infoTypeAccess>
        <infoType>
          <label>Telephony</label>
          <filter>filter</filter>
          <specFlags>FULL</specFlags>
        </infoType>
        <access>BLOCK</access>
      </infoTypeAccess>
    </presenceUserCLDefault>

  </delta:userDelta>
</delta:deltaUserList>
```

XML Schema Definition for bulk deletion of users

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/bulkdelete"
targetNamespace="http://xml.avaya.com/schema/bulkdelete"
          elementFormDefault="qualified" version="1.0" xmlns:xs="http://www.w3.org/
2001/XMLSchema" >

   <xs:element name="user" type="tns:xmlUserDelete" />
   <xs:element name="deleteType" type="tns:xmlDeleteType" />

   <xs:element name="deleteUsers">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="deleteType" type="tns:xmlDeleteType" maxOccurs="1"
minOccurs="1"/>
             <xs:element minOccurs="1" maxOccurs="unbounded" name="user"
type="tns:xmlUserDelete" />
        </xs:sequence>
    </xs:complexType>
   </xs:element>


   <xs:complexType name="xmlUserDelete">
       <xs:sequence>
           <xs:element name="loginName" minOccurs="1" maxOccurs="1">
               <xs:simpleType>
                   <xs:restriction base="xs:string">
                       <xs:maxLength value="128"></xs:maxLength>
                   </xs:restriction>
               </xs:simpleType>
           </xs:element>
           <xs:element name="id" type="xs:string" maxOccurs="1" minOccurs="0"></
xs:element>
       </xs:sequence>
   </xs:complexType>

  <xs:simpleType name="xmlDeleteType">
      <xs:restriction base="xs:string"></xs:restriction>
  </xs:simpleType>
</xs:schema>
```

Sample XML for bulk deletion of users

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:deleteUsers xmlns:tns="http://xml.avaya.com/schema/bulkdelete"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/bulkdelete UserProfileSchemaDefinitionForBulkDelete.xsd ">
  <tns:deleteType>soft</tns:deleteType>
  <tns:user>
    <tns:loginName>jmiller@avaya.com</tns:loginName>
  </tns:user>
</tns:deleteUsers>
```

XML Schema Definition for bulk import of elements

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://www.avaya.com/rts"
    xmlns="http://www.avaya.com/rts"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified" attributeFormDefault="unqualified">

    <!-- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"> -->
    <xs:element name="RTSElements">
```

```
        <xs:complexType>
            <xs:sequence>
                <xs:element name="ApplicationSystems" minOccurs="0"
                    maxOccurs="unbounded">
                    <xs:annotation>
                        <xs:documentation>
                            Application System Types
                        </xs:documentation>
                    </xs:annotation>
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="ApplicationSystem"
                                type="ApplicationSystem" maxOccurs="unbounded">
                            </xs:element>

                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="ApplicationSystemAssigns"
                    minOccurs="0" maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Source" type="Source"
                                minOccurs="1" maxOccurs="unbounded" />
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:complexType name="ApplicationSystem">
        <xs:annotation>
            <xs:documentation></xs:documentation>
        </xs:annotation>

        <xs:sequence>
            <xs:element name="Host" type="Host" minOccurs="1"
                maxOccurs="1">
            </xs:element>
            <xs:element name="ApplicationSystemType"
                type="ApplicationSystemType" minOccurs="1" maxOccurs="1">
            </xs:element>

           <xs:element name="SecureStoreData" type="SecureStoreData" minOccurs="0"
maxOccurs="1"/>

            <xs:element name="AccessPoints" minOccurs="0"
                maxOccurs="unbounded">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="AccessPoint"
                           type="AccessPoint" minOccurs="1" maxOccurs="unbounded" />
                    </xs:sequence>
                </xs:complexType>
            </xs:element>

            <xs:element name="Ports" minOccurs="0"
                maxOccurs="unbounded">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Port" type="Port"
                            minOccurs="1" maxOccurs="unbounded" />
                    </xs:sequence>
                </xs:complexType>
```

```
            </xs:element>

            <xs:element name="SNMPAttributes" type="SNMPAttributes" minOccurs="0"
                maxOccurs="1">
            </xs:element>

            <xs:element name="Attributes" minOccurs="0"
                maxOccurs="unbounded">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Attribute" type="Attribute"
                            minOccurs="1" maxOccurs="unbounded" />
                    </xs:sequence>
                </xs:complexType>
            </xs:element>

        </xs:sequence>

        <xs:attribute name="name" type="xs:string" use="required">
        </xs:attribute>

        <xs:attribute name="description" type="xs:string">
        </xs:attribute>

        <xs:attribute name="displaykey" type="xs:string"></xs:attribute>

        <xs:attribute name="isTrusted" type="xs:boolean"></xs:attribute>

    </xs:complexType>
    <xs:complexType name="SNMPAttributes">
        <xs:annotation>
            <xs:documentation></xs:documentation>
        </xs:annotation>
        <xs:attribute name="snmpVersion" type="snmpVersionType" use="required">
        </xs:attribute>

        <xs:attribute name="readCommunity" type="xs:string">
        </xs:attribute>

        <xs:attribute name="writeCommunity" type="xs:string">
        </xs:attribute>

        <xs:attribute name="userName" type="xs:string">
        </xs:attribute>

        <xs:attribute name="authenticationProtocol"
type="authenticationProtocolType">
        </xs:attribute>

        <xs:attribute name="authenticationPassword" type="xs:string">
        </xs:attribute>

        <xs:attribute name="privacyProtocol" type="privacyProtocolType">
        </xs:attribute>

        <xs:attribute name="privacyPassword" type="xs:string">
        </xs:attribute>

        <xs:attribute name="snmpRetries" type="xs:int" use="required">
        </xs:attribute>

        <xs:attribute name="snmpTimeout" type="xs:long" use="required">
        </xs:attribute>

        <xs:attribute name="deviceTypeName" type="xs:string"> </xs:attribute>
```

```
    <xs:attribute name="sysOid" type="xs:string">
    </xs:attribute>
</xs:complexType>

<xs:complexType name="Host">
    <xs:annotation>
        <xs:documentation></xs:documentation>
    </xs:annotation>

    <xs:attribute name="ipaddress" type="xs:string"
        use="required">
    </xs:attribute>

    <xs:attribute name="description" type="xs:string">
    </xs:attribute>

    <xs:attribute name="ostype" type="xs:string"></xs:attribute>
</xs:complexType>

<xs:complexType name="ApplicationSystemType">
    <xs:annotation>
        <xs:documentation></xs:documentation>
    </xs:annotation>

    <xs:attribute name="name" type="xs:string" use="required">
    </xs:attribute>

    <xs:attribute name="version" type="xs:string" use="required">
    </xs:attribute>

</xs:complexType>

<xs:complexType name="AccessPoint">
    <xs:annotation>
        <xs:documentation></xs:documentation>
    </xs:annotation>

    <xs:attribute name="name" type="xs:string" use="required">
    </xs:attribute>

    <xs:attribute name="description" type="xs:string">
    </xs:attribute>

    <xs:attribute name="displaykey" type="xs:string"></xs:attribute>

    <xs:attribute name="type" type="AccessPointType"
        use="required">
    </xs:attribute>

    <xs:attribute name="uri" type="xs:string"></xs:attribute>

    <xs:attribute name="host" type="xs:string" use="required">
    </xs:attribute>

    <xs:attribute name="port" type="xs:string"></xs:attribute>

    <xs:attribute name="protocol" type="xs:string"></xs:attribute>

    <xs:attribute name="loginid" type="xs:string"></xs:attribute>

    <xs:attribute name="password" type="xs:string"></xs:attribute>

    <xs:attribute name="containerType" type="ContainerType"></xs:attribute>
```

```
        <xs:attribute name="order" type="xs:int" use="required">
        </xs:attribute>

    </xs:complexType>

    <xs:complexType name="Port">
        <xs:annotation>
            <xs:documentation></xs:documentation>
        </xs:annotation>

        <xs:attribute name="name" type="xs:string" use="required">
        </xs:attribute>

        <xs:attribute name="description" type="xs:string">
        </xs:attribute>

       <xs:attribute name="protocol" type="xs:string" use="required"></xs:attribute>

        <xs:attribute name="port" type="xs:int" use="required"></xs:attribute>
    </xs:complexType>

    <xs:complexType name="Source">
        <xs:sequence>
            <xs:element name="Assignment" minOccurs="1"
                maxOccurs="unbounded">
                <xs:complexType>
                    <xs:attribute name="name" type="xs:string">
                    </xs:attribute>

                    <xs:attribute name="targetAppSystemName"
                        type="xs:string" use="required">
                    </xs:attribute>

                    <xs:attribute name="targetAppSystemTypeName"
                        type="xs:string" use="required">
                    </xs:attribute>

                    <xs:attribute name="targetAppSystemTypeVersion"
                        type="xs:string" use="required">
                    </xs:attribute>

                    <xs:attribute name="targetAppSystemHost"
                        type="xs:string" use="required">
                    </xs:attribute>

                    <xs:attribute name="priority" type="xs:int"></xs:attribute>
                </xs:complexType>
            </xs:element>
        </xs:sequence>

        <xs:attribute name="sourceApplicationSystemName"
            type="xs:string" use="required">
        </xs:attribute>

        <xs:attribute name="sourceAppSystemTypeName" type="xs:string"
            use="required">
        </xs:attribute>

        <xs:attribute name="sourceAppSystemTypeVersion" type="xs:string"
            use="required">
        </xs:attribute>

        <xs:attribute name="sourceAppSystemHost" type="xs:string"
            use="required">
        </xs:attribute>
```

```
    </xs:complexType>

    <xs:complexType name="Attribute">
        <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
        <xs:attribute name="value" type="xs:string" use="required"></xs:attribute>
        <!--  added for secure store integration. -->
        <xs:attribute name="isencrypted" type="xs:boolean" use="optional"
default="false"></xs:attribute>
    </xs:complexType>

    <xs:complexType name="SecureStoreData">
        <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
        <xs:attribute name="value" type="xs:string" use="required"></
xs:attribute>
    </xs:complexType>

    <xs:simpleType name="AccessPointType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="TrustManagement" />
            <xs:enumeration value="EMURL" />
            <xs:enumeration value="WS" />
            <xs:enumeration value="GUI" />
            <xs:enumeration value="Other" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="ContainerType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="JBOSS" />
            <xs:enumeration value="SIPAS" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="authenticationProtocolType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="MD5" />
            <xs:enumeration value="SHA" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="privacyProtocolType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="DES"/>
            <xs:enumeration value="3DES"/>
            <xs:enumeration value="AES128"/>
            <xs:enumeration value="AES192"/>
            <xs:enumeration value="AES256"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="snmpVersionType">
        <xs:restriction base="xs:int">
            <xs:enumeration value="1"/>
            <xs:enumeration value="3"/>
        </xs:restriction>
    </xs:simpleType>

</xs:schema>
```

Sample XML for bulk import of elements

```
<?xml version="1.0" encoding="UTF-8"?>
<RTSElements xsi:schemaLocation="http://www.avaya.com/rts ApplicationSystems.xsd "
xmlns="http://www.avaya.com/rts" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
    <ApplicationSystems>
```

```
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test1">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test2">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test3">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test4">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test5">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test6">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test7">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test8">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test9">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test10">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Tes11t">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test12">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test13">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
```

```
        <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test14">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
    </ApplicationSystems>
</RTSElements>
```

XML Schema Definition for bulk import of Session Manager profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:smgr="http://xml.avaya.com/schema/import"
            targetNamespace="http://xml.avaya.com/schema/import_sessionmanager"
            elementFormDefault="qualified">

<xsd:import namespace="http://xml.avaya.com/schema/import"
            schemaLocation="userimport.xsd"/>

<xsd:complexType name="SessionManagerCommProfXML">

    <xsd:complexContent>
        <xsd:extension base="smgr:xmlCommProfileType" >

             <xsd:sequence>
                 <xsd:element name="primarySM" type="xsd:string"/>
              <xsd:element name="secondarySM" type="xsd:string" minOccurs="0" />
              <xsd:element name="originationAppSequence" type="xsd:string"
minOccurs="0" />
              <xsd:element name="terminationAppSequence" type="xsd:string"
minOccurs="0" />
              <xsd:element name="confFactorySet" type="xsd:string" minOccurs="0" />
              <xsd:element name="survivabilityServer" type="xsd:string"
minOccurs="0" />
              <xsd:element name="homeLocation" type="xsd:string"  />

            </xsd:sequence>

        </xsd:extension>
     </xsd:complexContent>
 </xsd:complexType>

</xsd:schema>
```

Sample XML for bulk import of Session Manager profiles

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd ">

    <!-- User Record for: 5555555@domain.com -->
    <tns:user>

(Other user elements are required here - consult the main user record XML schema
reference)

    <!-- This is the password for any SIP endpoints (phones)
            associated with the user's Session Manager Profile -->
        <commPassword>123456</commPassword>

(Other user elements may be required here - consult the main user record XML schema
reference)

        <!-- Here, a Communication Profile is defined for the user -->
```

```
       <commProfileSet>
           <commProfileSetName>Primary</commProfileSetName>
                <isPrimary>true</isPrimary>

<!-- The user must be given one or more handles of type “SIP”
     to associate SIP devices with the Session Manager
     Profile.  In this case, a SIP phone will be registered
     with a Session Manager as 5555555@domain.com -->
                <handleList>
                <handle>
                <handleName>5555555</handleName>
                <handleType>sip</handleType>
                <handleSubType>username</handleSubType>
                <domainName>domain.com</domainName>
                </handle>
                </handleList>

        <!-- Here, one or more product-specific profiles may be
                  Defined -->
<commProfileList>

<!-- A Session Manager Profile is defined to associate
     the SIP phone, 5555555@domain.com, with a primary
     and secondary Session Mananger instance
     (“Primary SM” and “Secondary SM”),
     origination and termination application
     sequences (both are “Sequence to My CM”),
     a Survivability Server (“BSM”), and the user
     is given the Home Location, “My Home” -->
                <commProfile xsi:type="sm:SessionManagerCommProfXML"
 xmlns:sm="http://xml.avaya.com/schema/import_sessionmanager">
                  <commProfileType>SessionManager</commProfileType>
                       <sm:primarySM>Primary SM</sm:primarySM>
                       <sm:secondarySM>Secondary SM</sm:secondarySM>
                    <sm:terminationAppSequence>Sequence to My CM
        </sm:terminationAppSequence>
                       <sm:originationAppSequence>Sequence to My CM
</sm:originationAppSequence>

<confFactorySet>EngeeringDepartmentConferenceSet</confFactorySet>

<sm:survivabilityServer>BSM
</sm:survivabilityServer>
                     <sm:homeLocation>My Home</sm:homeLocation>
              </commProfile>


<!-- A CM Station Profile is associated with this
     Communication Profile.  The application
     sequence, “Sequence to My CM”, invoked by
     Session Manager for calls to and from
     5555555@domain.com, sequences calls to the
     CM, “My CM”. SIP devices associated
     with this Communication Profile are associated
     with the CM Station that has number 555-5555. The
     CM Station, 555-5555, already exists on the CM, so the
     “useExistingExtension” element has value “true”. -->
<commProfile xsi:type="ipt:xmlStationProfile"
                       xmlns:ipt="http://xml.avaya.com/schema/import_csm_cm">
                    <commProfileType>CM</commProfileType>
                    <ipt:cmName>My CM</ipt:cmName>
                    <ipt:useExistingExtension>true</ipt:useExistingExtension>
                    <ipt:extension>5555555</ipt:extension>
              </commProfile>
```

```
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of endpoint profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:one="http://
xml.avaya.com/schema/import" elementFormDefault="qualified"
targetNamespace="http://xml.avaya.com/schema/import_csm_cm" xmlns:csm="http://
xml.avaya.com/schema/import_csm_cm">
<xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>

<!--Changes in xsd file need to generate jaxb src using this xsd-->
<xs:complexType name="xmlStationProfile">
    <xs:complexContent>
           <xs:extension base="one:xmlCommProfileType" >
            <xs:sequence>

              <!-- CM Name as it appears under 'Applications/Application Management/
Entities -->
                <xs:element name="cmName" type="xs:string" maxOccurs="1"
minOccurs="1"/>
                <xs:element name="prefHandleId" type="xs:string" maxOccurs="1"
minOccurs="0"/>
               <!-- 'true' if already created extension is to be used.  'false' if
available extension is to be used. -->
                <xs:element name="useExistingExtension" type="xs:boolean"
maxOccurs="1" minOccurs="0"/>

                <!-- Extension Range which will be used to create Station using
available extension within given range -->
                <xs:element name="extensionRange" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                           <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|([0-9]+([\.\-]
[0-9]+)*:[0-9]+([\.\-][0-9]+)*)"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

             <!-- Station extension number that need to be assigned to the user. -->
                <xs:element name="extension" maxOccurs="1" minOccurs="1">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|[nN][eE][xX]
[tT]"/>
                       </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Template name to be used to create station. Values defined in
Template will be used if not provided. -->
                <xs:element name="template" type="xs:string" maxOccurs="1"
minOccurs="0"/>

                <!-- Specifies the set type of the station  -->
                <xs:element name="setType" type="xs:string" maxOccurs="1"
minOccurs="0"/>

                <!-- Security code for station. Value can be digit only.  -->
                <xs:element name="securityCode" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
```

```
                        <xs:restriction base="xs:string">
                          <xs:pattern value="[0-9]*"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <!-- Valid values for port   -->
                <!--01 to 64  First and second numbers are the cabinet number  -->
                <!--A to E  Third character is the carrier  -->
                <!--01 to 20  Fourth and fifth characters are the slot number  -->
              <!--01 to 32  Sixth and seventh characters are the circuit number  -->
                <!--x or X  Indicates that there is no hardware associated with the
port assignment since the switch was set up, and the administrator expects that the
extension would have a non-IP set. Or, the extension had a non-IP set, and it
dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony
(CTI) stations, as well as for SBS Extensions.  -->
              <!--IP  Indicates that there is no hardware associated with the port
assignment since the switch was set up, and the administrator expects that the
extension would have an IP set. This is automatically entered for certain IP station
set types, but you can enter for a DCP set with softphone permissions. This changes
to the s00000 type when the set registers.  -->
             <xs:element name="port" type="xs:string" maxOccurs="1" minOccurs="0" /
>

               <!-- Whether the station should be deleted if it unassigned from the
user. -->
                <xs:element name="deleteOnUnassign" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

                <!-- Whether the endpoint name on CM should be overridden with the
value in User. -->
                <xs:element name="overRideEndpointName" type="xs:boolean"
maxOccurs="1" minOccurs="0"/>

               <!-- true/false for Enhanced Callr-Info display for 1-line phones -->
                <xs:element name="enhCallrInfodisplay" type="xs:boolean"
maxOccurs="1" minOccurs="0"/>

                <!-- true/false to enable/disable lock messages feature. -->
                <xs:element name="lockMessages" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

              <!-- A coverage path is a prioritized sequence of extensions to which
your voice system will route an unanswered call. -->
               <!-- Valid values: CM 5.2 - Path Number between 1-2000, time of day
table, t1-t999, or blank. -->
               <!-- Valid values: CM 6.0 - Path Number between 1-9999, time of day
table, t1-t999, or blank. -->
                <xs:element name="coveragePath1" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:pattern value="(t[1-9][0-9]{0,2})|([1-9][0-9]{0,3})"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

              <!-- A coverage path is a prioritized sequence of extensions to which
your voice system will route an unanswered call. -->
               <!-- Valid values: CM 5.2 - Path Number between 1-2000, time of day
table, t1-t999, or blank. -->
               <!-- Valid values: CM 6.0 - Path Number between 1-9999, time of day
table, t1-t999, or blank. -->
                <xs:element name="coveragePath2" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
```

```
                        <xs:restriction base="xs:string">
                          <xs:pattern value="(t[1-9][0-9]{0,2})|([1-9][0-9]{0,3})"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

               <!-- The extension the system should hunt to for this telephone when
the telephone is busy. A station hunting chain can be created by assigning a hunt-
to station to a series of telephones.  -->
                <xs:element name="huntToStation" type="xs:string" maxOccurs="1"
minOccurs="0" />

                <!-- Provides for partitioning of attendant groups and/or stations
and trunk groups. -->
                <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
                <!-- Valid values: 1 to 100 -->
                <xs:element name="tn" maxOccurs="1" minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:int">
                            <xs:minInclusive value="0" />
                            <xs:maxInclusive value="100" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
                <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
                <!-- Valid values: 0 to 995 -->
                <xs:element name="cor" maxOccurs="1" minOccurs="0">
                      <xs:simpleType>
                        <xs:restriction base="xs:int">
                              <xs:minInclusive value="0"/>
                              <xs:maxInclusive value="995"/>
                        </xs:restriction>
                      </xs:simpleType>
                </xs:element>

                <!-- Class of Service lets you define groups of users and control
those groups' access to features -->
                <!-- Valid values: 1 to 15 -->
                <xs:element name="cos" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:int">
                            <xs:minInclusive value="0" />
                            <xs:maxInclusive value="15" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="xmobileType" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="EC500"/>
                            <xs:enumeration value="DECT"/>
                            <xs:enumeration value="IPDECT"/>
                            <xs:enumeration value="PHS"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="mappingMode" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
```

```
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="termination"/>
                          <xs:enumeration value="origination"/>
                          <xs:enumeration value="both"/>
                          <xs:enumeration value="none"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="configurationSet" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="|[1-9]|[0-9][1-9]"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="mobilityTrunkGroup" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:pattern value="aar|ars|[1-9]|[1-9][0-9]|[1-9]([0-9])
{2}|[1]([0-9]){3}|2000"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="dialPrefix" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="([0-9]*#){0,4}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="cellPhoneNumber" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{0,15}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="musicSource" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:int">
                          <xs:minInclusive value="1" />
                          <xs:maxInclusive value="250" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="tests" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="dataModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- Controls the behavior of speakerphones. -->
                <xs:element name="speakerphone" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="none"/>
                          <xs:enumeration value="1-way"/>
                          <xs:enumeration value="2-way"/>
                        </xs:restriction>
```

```
                    </xs:simpleType>
                </xs:element>

                <!-- The language that displays on stations -->
                <!-- Time of day is displayed in 24-hour format (00:00 - 23:59) for
all languages except English, which is displayed in 12-hour format (12:00 a.m. to
11:59 p.m.). -->
                <!-- unicode: Displays English messages in a 24-hour format . If no
Unicode file is installed, displays messages in English by default. -->
                <xs:element name="displayLanguage" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="english"/>
                            <xs:enumeration value="french"/>
                            <xs:enumeration value="italian"/>
                            <xs:enumeration value="spanish"/>
                            <xs:enumeration value="unicode"/>
                            <xs:enumeration value="unicode2"/>
                            <xs:enumeration value="unicode3"/>
                            <xs:enumeration value="unicode4"/>
                            <xs:enumeration value="user-defined"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Defines the personalized ringing pattern for the station.
                   Personalized Ringing allows users of some telephones to have one
of 8 ringing patterns for incoming calls.
                    For virtual stations, this field dictates the ringing pattern
on its mapped-to physical telephone.
                -->
                <!-- L = 530 Hz, M = 750 Hz, and H = 1060 Hz -->
                <!-- Valid Entries  Usage
                    1  MMM (standard ringing)
                    2  HHH
                    3  LLL
                    4  LHH
                    5  HHL
                    6  HLL
                    7  HLH
                    8  LHL
                 -->
                <xs:element name="personalizedRingingPattern" maxOccurs="1"
minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:int">
                            <xs:minInclusive value="0" />
                            <xs:maxInclusive value="8" />
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>


              <!-- The Message Lamp Extension associated with the current extension
-->
                <xs:element name="messageLampExt" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]+([\.\-][0-9]+)*"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Enables or disables the mute button on the station. -->
               <xs:element name="muteButtonEnabled" type="xs:boolean" maxOccurs="1"
```

```
minOccurs="0" />

                <!--
                 When used with Multi-media Call Handling, indicates which extension
is
                   assigned to the data module of the multimedia complex. Users can
dial
                    this extension to place either a voice or a data call, and voice
                    conversion, coverage, and forwarding apply as if the call were
made to
                    the 1-number.
                -->
                <!--
                    Valid Entry Usage A valid BRI data extension For MMCH, enter the
                    extension of the data module that is part of this multimedia
complex.
                    H.323 station extension For 4600 series IP Telephones, enter the
                    corresponding H.323 station. For IP Softphone, enter the
corresponding
                  H.323 station. If you enter a value in this field, you can register
                    this station for either a road-warrior or telecommuter/Avaya IP
Agent
                    application. blank Leave this field blank for single-connect IP
                    applications.
                -->
                <xs:element name="mediaComplexExt" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]+([\.\-][0-9]+)*"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Whether this is IP soft phone. -->
                <xs:element name="ipSoftphone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                    Survivable GK Node Name Identifies the existence of other H.323
                   gatekeepers located within gateway products that offer survivable
call
                   features. For example, the MultiTech MVPxxx-AV H.323 gateway family
                   and the SLS function within the H.248 gateways. When a valid IP node
                    name is entered into this field, Communication Manager adds the IP
                    address of this gateway to the bottom of the Alternate Gatekeeper
List
                    for this IP network region. As H.323 IP stations register with
                   Communication Manager, this list is sent down in the registration
                   confirm message. This allows the IP station to use the IP address of
                    this Survivable Gatekeeper as the call controller of last resort to
                    register with. Available only if the station type is an H.323
station
                    (46xxor 96xx models).
                    Valid Entry             Usage
                    Valid IP node name        Any valid previously-administered IP
node name.
                    blank                    There are no external gatekeeper nodes
within a customer's network. This is the default value.
                -->
                <xs:element name="survivableGkNodeName" type="xs:string"
maxOccurs="1" minOccurs="0" />

                <!--
                    Sets a level of restriction for stations to be used with the
                   survivable dial plan to limit certain users to only to certain types
```

```
                  of calls. You can list the restriction levels in order from the most
                     restrictive to least restrictive. Each level assumes the calling
                     ability of the ones above it. This field is used by PIM module
of the
                  Integrated Management to communicate with the Communication Manager
                  administration tables and obtain the class of service information.
PIM
                     module builds a managed database to send for Standard Local
                  Survivability (SLS) on the H.248 gateways. Available for all analog
                     and IP station types.

                     Valid Entries         Usage
                     emergency             This station can only be used to place
emergency calls.
                     internal             This station can only make intra-switch
calls. This is the default.
                     local                 This station can only make calls that are
defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's
routing tables.
                     toll                 This station can place any national toll
calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's
routing tables.
                       unrestricted        This station can place a call to any number
defined in the Survivable Gateway Call Controller's routing tables. Those strings
marked as deny are also denied to these users.
                -->
                <xs:element name="survivableCOR" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="emergency"/>
                            <xs:enumeration value="internal"/>
                            <xs:enumeration value="local"/>
                            <xs:enumeration value="toll"/>
                            <xs:enumeration value="unrestricted"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    Designates certain telephones as not being allowed to receive
incoming
                 trunk calls when the Media Gateway is in survivable mode. This field
                    is used by the PIM module of the Integrated Management to
successfully
                   interrogate the Communication Manager administration tables and
obtain
                    the class of service information. PIM module builds a managed
database
                   to send for SLS on the H.248 gateways. Available for all analog
and IP
                    station types.

                    Valid Entry         Usage
                       true            Allows this station to be an incoming trunk
destination while the Media Gateway is running in survivability mode. This is the
default.
                        false             Prevents this station from receiving
incoming trunk calls when in survivable mode.

                -->
                <xs:element name="survivableTrunkDest" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!-- Enter the complete Voice Mail Dial Up number. -->
                <xs:element name="voiceMailNumber" maxOccurs="1" minOccurs="0" >
```

```
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{0,23}[0-9]|[*]|[#]|~p|~w|~W|~m|
~s"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Analog telephones only. -->
                <!--
                Valid entries         Usage
                        true         Enter true if this telephone is not located in
the same building with the system. If you enter true, you must complete R Balance
Network.
                       false         Enter false if the telephone is located in the
same building with the system.
                 -->
              <xs:element name="offPremisesStation" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- If a second line on the telephone is administered on the I-2
channel, enter analog. Otherwise, enter data module if applicable or none. -->
                <xs:element name="dataOption" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="analog"/>
                            <xs:enumeration value="data-module"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <xs:element name="displayModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- if led or neon then messageLampExt should be enable otherwise
its blank -->
                <xs:element name="messageWaitingIndicator" maxOccurs="1"
minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="led"/>
                            <xs:enumeration value="neon"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

              <!-- Enter true to use this station as an endpoint in a remote office
configuration. -->
               <xs:element name="remoteOfficePhone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- Defines the source for Leave Word Calling (LWC) messages. -->
                <!--
                Valid entries            Usage
                    audix                If LWC is attempted, the messages are
stored in AUDIX.
                     spe                If LWC is attempted, the messages are stored
in the system processing element (spe).
                   none               If LWC is attempted, the messages are not stored.

                 -->
```

```
                <xs:element name="lwcReception" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="audix"/>
                            <xs:enumeration value="msa"/>
                            <xs:enumeration value="spe"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    Enter true to allow internal telephone users to leave short LWC
messages
                   for this extension. If the system has hospitality, enter true for
                  guest-room telephones if the extension designated to receive failed
                  wakeup messages should receive LWC messages that indicate the wakeup
                    calls failed. Enter true if LWC Reception is audix.
                -->
                <xs:element name="lwcActivation" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="lwcLogExternalCalls" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="cdrPrivacy" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="redirectNotification" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="perButtonRingControl" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="bridgedCallAlerting" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="bridgedIdleLinePreference" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="confTransOnPrimaryAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
              <xs:element name="customizableLabels" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="expansionModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                 <xs:element name="ipVideoSoftphone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="activeStationRinging" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="single"/>
                            <xs:enumeration value="continuous"/>
                            <xs:enumeration value="if-busy-single"/>
                            <xs:enumeration value="silent"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Defines how call rings to the telephone when it is on-hook. -->
                <!--
                    Valid entries             Usage
                    continuous                 Enter continuous to cause all calls
to this telephone to ring continuously.
                    if-busy-single             Enter if-busy-single to cause calls
to this telephone to ring continuously when the telephone is off-hook and idle and
calls to this telephone to
                                              receive one ring cycle and then ring
silently when the telephone is off-hook and active.
                    silent-if-busy             Enter silent-if-busy to cause calls
```

```
to ring silently when this station is busy.
                    single                    Enter single to cause calls to this
telephone to receive one ring cycle and then ring silently.
                -->
               <xs:element name="idleActiveRinging" type="xs:string" maxOccurs="1"
minOccurs="0" /> <!-- not found in xhtml -->

                <!-- Must be set to true when the Type field is set to H.323. -->
                <xs:element name="switchhookFlash" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

               <!-- If this field is true, the short switch-hook flash (50 to 150)
from a 2500-type set is ignored. -->
              <xs:element name="ignoreRotaryDigits" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                    H.320 Conversion - Valid entries are true and false (default).
This field is
                   optional for non-multimedia complex voice stations and for Basic
                    multimedia complex voice stations. It is mandatory for Enhanced
                    multimedia complex voice stations. Because the system can only
handle
                   a limited number of conversion calls, you might need to limit the
                    number of telephones with H.320 conversion. Enhanced multimedia
                    complexes must have this flag set to true.
                -->
                            <xs:element name="h320Conversion" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

               <!--
                  The service link is the combined hardware and software multimedia
                    connection between an Enhanced mode complex's H.320 DVC system
and the
                Avaya DEFINITY Server which terminates the H.320 protocol. A service
                    link is never used by a Basic mode complex H.320 DVC system.
                    Connecting a service link will take several seconds. When the
service
                  link is connected, it uses MMI, VC and system timeslot resources.
When
                 the service link is disconnected it does not tie up any resources.
                    The
                    Service Link Mode can be administered as either 'as-needed' or
                  'permanent' as described below: - As-Needed - Most non-call center
                    multimedia users will be administered with this service link
mode. The
                    as-needed mode provides the Enhanced multimedia complex with a
                 connected service link whenever a multimedia call is answered by the
                   station and for a period of 10 seconds after the last multimedia
call
                  on the station has been disconnected. Having the service link stay
                  connected for 10 seconds allows a user to disconnect a multimedia
call
                 and then make another multimedia call without having to wait for the
                    service link to disconnect and re-establish. - Permanent -
Multimedia
                    call center agents and other users who are constantly making or
                   receiving multimedia calls might want to be administered with this
                 service link mode. The permanent mode service link will be connected
                    during the station's first multimedia call and will remain in a
                    connected state until the user disconnects from their PC's
multimedia
                  application or the Avaya DEFINITY Server restarts. This provides a
                    multimedia user with a much quicker video cut-through when
answering a
```

```
                  multimedia call from another permanent mode station or a multimedia
                 call that has been early answered. ● Multimedia Mode - There are two
                    multimedia modes, Basic and Enhanced, as
                -->
                <xs:element name="serviceLinkMode" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="as-needed"/>
                            <xs:enumeration value="permanent"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    There are two multimedia modes, Basic and Enhanced, as described
                    below:
                    Basic - A Basic multimedia complex consists of a
                    BRI-connected multimedia-equipped PC and a non-BRI-connected
                  multifunction telephone set. When in Basic mode, users place voice
                  calls at the multifunction telephone and multimedia calls from the
                    multimedia equipped PC. Voice calls will be answered at the
                 multifunction telephone and multimedia calls will alert first at the
                   PC and if unanswered will next alert at the voice station if it is
                    administered with H.320 enabled. A Basic mode complex has limited
                    multimedia feature capability.
                    Enhanced - An Enhanced multimedia complex consists of a
                    BRI-connected multimedia-equipped PC and a non-BRI-connected
                  multifunction telephone. The Enhanced mode station acts as though
the
                    PC were directly connected to the multifunction telephone; the
service
                    link provides the actual connection between the Avaya DEFINITY
Server
                    and the PC. Thus, voice and multimedia calls are originated and
                  received at the telephone set. Voice and multimedia call status are
                 also displayed at the telephone set. An Enhanced mode station allows
                    multimedia calls to take full advantage of most call control
features
                -->
                <xs:element name="multimediaMode" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="basic"/>
                            <xs:enumeration value="enhanced"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

              <!-- Controls the auditing or interrogation of a served user's message
waiting indicator (MWI).
                Valid entries             Usage
                    fp-mwi                 Use if the station is a served user of
an fp-mwi message center.
                    qsig-mwi              Use if the station is a served user of a
qsig-mwi message center.
                    blank                  Leave blank if you do not want to audit
the served user's MWI or
                                          if the user is not a served user of either
an fp-mwi or qsig-mwi message center.
                 -->
                <xs:element name="mwiServedUserType" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="fp-mwi"/>
                            <xs:enumeration value="qsig-mwi"/>
```

```
                            <xs:enumeration value="sip-adjunct"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- The AUDIX associated with the station.
                    Must contain a user-defined adjunct name that was previously
administered.
                -->
                        <xs:element name="audixName" type="xs:string" maxOccurs="1"
minOccurs="0" />

                <!--
                    Automatic Moves allows a DCP telephone to be unplugged from one
                    location and moved to a new location without additional
Communication
                    Manager administration. Communication Manager automatically
associates
                    the extension to the new port.

                    **********CAUTION**********
                    When a DCP telephone is unplugged and
                    moved to another physical location, the Emergency Location
Extension
                    field must be changed for that extension or the USA Automatic
Location
                  Identification data base must be manually updated. If the Emergency
                    Location Extension field is not changed or if the USA Automatic
                   Location Identification data base is not updated, the DID number
sent
                 to the Public Safety Network could send emergency response personnel
                    to the wrong location.
                Valid entries            Usage
                    always             Enter always and the DCP telephone can be
moved anytime without
                                      additional administration by unplugging from one
location and plugging
                                       into a new location.
                     once            Enter once and the DCP telephone can be unplugged
and plugged into a
                                       new location once. After a move, the field is
set to done the next time that
                                       routine maintenance runs on the DCP telephone.
                                       Use once when moving a large number of DCP
telephones so each
                                       extension is removed from the move list. Use
once to prevent automatic
                                       maintenance replacement.
                    no                    Enter no to require administration in order
to move the DCP telephone.
                    done                Done is a display-only value. Communication
Manager sets the field to
                                       done after the telephone is moved and routine
maintenance runs on the
                                       DCP telephone.
                    error               Error is a display-only value. Communication
Manager sets the field to
                                      error, after routine maintenance runs on the DCP
telephone, when a
                                       non-serialized telephone is set as a movable
telephone.
                -->
                <xs:element name="automaticMoves" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
```

```
                            <xs:enumeration value="always"/>
                            <xs:enumeration value="no"/>
                            <xs:enumeration value="once"/>
                          </xs:restriction>
                      </xs:simpleType>
                  </xs:element>


                  <!--
                      Tells Communication Manager how to handle emergency calls from
the IP
                      telephone.
                                        **********CAUTION**********
                                                              An Avaya IP endpoint can dial
                      emergency calls (for example, 911 calls in the U.S.). It only
reaches
                     the local emergency service in the Public Safety Answering Point
area
                      where the telephone system has local trunks. Please be advised
that an
                     Avaya IP endpoint cannot dial to and connect with local emergency
                     service when dialing from remote locations that do not have local
                    trunks. Do not use an Avaya IP endpoint to dial emergency numbers
for
                   emergency services when dialing from remote locations. Avaya Inc. is
                    not responsible or liable for any damages resulting from misplaced
                      emergency calls made from an Avaya endpoint. Your use of this
product
                      indicates that you have read this advisory and agree to use an
                      alternative telephone to dial all emergency calls from remote
                      locations. Please contact your Avaya representative if you have
                      questions about emergency calls from IP telephones. Available
only if
                      the station is an IP Softphone or a remote office station.

                      Valid entries                 Usage
                      as-on-local                Type as-on-local to achieve the
following results:
                                                   If the administrator chooses to leave
the Emergency Location
                                                   Extension fields (that correspond to
this station's IP address) on
                                                  the IP Address Mapping screen blank, the
value as-on-local
                                                   sends the extension entered in the
Emergency Location
                                                   Extension field in the Station screen
to the Public Safety
                                                   Answering Point (PSAP).
                                                   If the administrator populates the IP
Address Mapping screen with
                                                  emergency numbers, the value as-on-local
functions as follows:
                                                   - If the Emergency Location Extension
field in the Station screen
                                                   is the same as the Emergency Location
Extension field in the
                                                  IP Address Mapping screen, the value as-
on-local sends the
                                                  extension to the Public Safety Answering
Point (PSAP).
                                                   - If the Emergency Location Extension
field in the Station screen
                                                  is different from the Emergency Location
Extension field in the
```

```
                                        IP Address Mapping screen, the value as-
on-local sends the
                                        extension in the IP Address Mapping
screen to the Public Safety
                                        Answering Point (PSAP).

                    block               Enter block to prevent the completion
of emergency calls. Use this entry
                                        for users who move around but always
have a circuit-switched telephone
                                        nearby, and for users who are farther
away from the Avaya S8XXX Server
                                       than an adjacent area code served by the
same 911 Tandem office.
                                        When users attempt to dial an emergency
call from an IP Telephone and
                                        the call is blocked, they can dial 911
from a nearby circuit-switched
                                        telephone instead.

                    cesid               Enter cesid to allow Communication
Manager to send the CESID
                                       information supplied by the IP Softphone
to the PSAP. The end user
                                        enters the emergency information into
the IP Softphone.
                                        Use this entry for IP Softphones with
road warrior service that are near
                                        enough to the Avaya S8XXX Server that
an emergency call routed over
                                        the it's trunk reaches the PSAP that
covers the server or switch.
                                        If the server uses ISDN trunks for
emergency calls, the digit string is the
                                        telephone number, provided that the
number is a local direct-dial number
                                       with the local area code, at the physical
location of the IP Softphone. If the
                                        server uses CAMA trunks for emergency
calls, the end user enters a
                                      specific digit string for each IP Softphone
location, based on advice from
                                       the local emergency response personnel.

                    option              Enter option to allow the user to
select the option (extension, block, or
                                        cesid) that the user selected during
registration and the IP Softphone
                                       reported. Use this entry for extensions
that can be swapped back and
                                      forth between IP Softphones and a telephone
with a fixed location.
                                       The user chooses between block and cesid
on the softphone. A DCP or
                                       IP telephone in the office automatically
selects extension.
                -->
                <xs:element name="remoteSoftphoneEmergencyCalls" maxOccurs="1"
minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="as-on-local"/>
                            <xs:enumeration value="block"/>
                            <xs:enumeration value="cesid"/>
                            <xs:enumeration value="option"/>
```

```
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <!--
                  This field allows the system to properly identify the location of a
                  caller who dials a 911 emergency call from this station. An entry in
                     this field must be of an extension type included in the dial
plan, but
                  does not have to be an extension on the local system. It can be a UDP
                     extension. The entry defaults to blank. A blank entry typically
would
                    be used for an IP softphone dialing in through PPP from somewhere
                   outside your network. If you populate the IP Address Mapping screen
                     with emergency numbers, the feature functions as follows: If the
                   Emergency Location Extension field in the Station screen is the same
                    as the Emergency Location Extension field in the IP Address Mapping
                     screen, the feature sends the extension to the Public Safety
Answering
                     Point (PSAP). If the Emergency Location Extension field in the
Station
                     screen is different from the Emergency Location Extension field
in the
                   IP Address Mapping screen, the feature sends the extension in the IP
                    Address Mapping screen to the Public Safety Answering Point (PSAP).
                -->
               <xs:element name="emergencyLocationExt" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]+([\.\-][0-9]+)*"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    A softphone can register no matter what emergency call handling
settings
                     the user has entered into the softphone. If a softphone dials
911, the
                    administered Emergency Location Extension is used. The softphone's
                   user-entered settings are ignored. If an IP telephone dials 911, the
                    administered Emergency Location Extension is used. If a call center
                     agent dials 911, the physical station extension is displayed,
                     overriding the administered LoginID for ISDN Display . Does not
apply
                    to SCCAN wireless telephones, or to extensions administered as type
                     h.323.
                -->
                <xs:element name="alwaysUse" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

              <!-- Activates or deactivates Precedence Call Waiting for this station
-->
                <xs:element name="precedenceCallWaiting" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                  Enables or disables automatic selection of any idle appearance for
                     transferred or conferenced calls. Communication Manager first
attempts
                   to find an idle appearance that has the same extension number as the
                    call being transferred or conferenced has. If that attempt fails,
                     Communication Manager selects the first idle appearance.
                -->
```

```
                              <xs:element name="autoSelectAnyIdleAppearance"
type="xs:boolean" maxOccurs="1" minOccurs="0" />

                <!--
                  Allows or denies users in the telephone's Coverage Path to retrieve
                     Leave Word Calling (LWC) messages for this telephone. Applies
only if
                     the telephone is enabled for LWC Reception.
                -->

                <xs:element name="coverageMsgRetrieval" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <!--
                  In EAS environments, the auto answer setting for the Agent LoginID
can
                     override a station's setting when an agent logs in.
                     Valid Entry            Usage
                     all                 All ACD and non-ACD calls terminated to an
idle station cut through immediately.
                                         Does not allow automatic hands-free answer
for intercom calls. With non-ACD calls,
                                         the set is also rung while the call is cut
through. The ring can be prevented by activating
                                        the ringer-off feature button when the Allow
Ringer-off with Auto-Answer is enabled for the system.
                      acd                Only ACD split /skill calls and direct agent
calls to auto answer. Non-ACD calls terminated to a station ring audibly.
                                         For analog stations, the station is off-hook
and idle, only the ACD split/skill calls and direct agent calls
                                          auto answer; non-ACD calls receive busy
treatment. If the station is active on an ACD call and
                                          a non-ACD call arrives, the Agent receives
call-waiting tone.
                     none                All calls terminated to this station receive
an audible ringing treatment.
                    icom                Allows a telephone user to answer an intercom
call from the same intercom group without pressing the intercom
button.
                -->
                <xs:element name="autoAnswer" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="acd"/>
                            <xs:enumeration value="all"/>
                            <xs:enumeration value="icom"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    Enables or disables data restriction that is used to prevent
tones, such as call-waiting tones, from interrupting data calls.
                    Data restriction provides permanent protection and cannot be
changed by the telephone user. Cannot be assigned if Auto Answer
                      is administered as all or acd. If enabled, whisper page to this
station is denied.
                 -->
                <xs:element name="dataRestriction" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                    Indicates which call appearance is selected when the user lifts
the handset and there is an incoming call.
                    Valid Entry                  Usage
```

```
                    true                          The user connects to an idle call
appearance instead of the ringing call.
                    false                         The Alerting Appearance Preference
is set and the user connects to the ringing call appearance.
                 -->
                <xs:element name="idleAppearancePreference" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    enable/disable call waiting for this station
                -->
                <xs:element name="callWaitingIndication" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    Attendant call waiting allows attendant-originated or attendant-
extended calls to a busy
                   single-line telephone to wait and sends distinctive call-waiting
tone to the single-line user.
                    Enable/disable attendant call waiting
                 -->
                <xs:element name="attCallWaitingIndication" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    Enter true so the telephone can receive the 3 different types
of ringing patterns which identify the type of incoming calls.
                     Distinctive ringing might not work properly for off-premises
telephones. -->
                <xs:element name="distinctiveAudibleAlert" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    Valid Entries            Usage
                    true                   Restricts the last idle call appearance
used for incoming priority calls and outgoing call originations only.
                    false                   Last idle call appearance is used for
incoming priority calls and outgoing call originations.
                 -->
                <xs:element name="restrictLastAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    Valid entries            Usage
                    true                    Analog disconnect signal is sent
automatically to the port after a call terminates. Analog devices
                                            (such as answering machines and
speakerphones) use this signal to turn the devices off after a call terminates.
                  false                   Hunt group agents are alerted to incoming
calls. In a hunt group environment, the disconnect
                                           signal blocks the reception of zip tone
and incoming call notification by an auto-answer station when a call
                                            is queued for the station.
                 -->
              <xs:element name="adjunctSupervision" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                        Send Calling Number.
                        Valid Entries         Usage
                        y                     All outgoing calls from the station
will deliver the Calling Party Number
                                           (CPN) information as "Presentation Allowed."
                      n                     No CPN information is sent for the call
                       r                    Outgoing non-DCS network calls from the
```

```
station will deliver the Calling
                                                Party Number information as "Presentation
Restricted."
                 -->
                <xs:element name="perStationCpnSendCallingNumber" maxOccurs="1"
minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="r"/>
                            <xs:enumeration value="n"/>
                            <xs:enumeration value="y"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                   Appears on the Station screen for analog telephones, only if the
Without Flash field in the
                    ANALOG BUSY AUTO CALLBACK section of the Feature-Related System
Parameters
                  screen is set to true. The Busy Auto Callback without Flash field
then defaults to true for all analog
                    telephones that allow Analog Automatic Callback.
                    Set true to provide automatic callback for a calling analog
station without flashing the hook.
                 -->
                <xs:element name="busyAutoCallbackWithoutFlash" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!-- Provides audible message waiting. -->
                <xs:element name="audibleMessageWaiting" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!-- Provides extended local calls
               Extended Local Calls (ELC) allows DCP and H.323 stations to use SIP
sequenced applications.  The feature works by routing calls
                involving those stations over SIP IMS trunks.  In other words, CM
is applying the half-call model to those stations.
                That also has the side effect that features which work differently
under the half-call model than under the usual (full-call) model
                also work differently for ELC stations.
              The Extended Local Calls feature is administrable per station.  We're
allowing stations that always use SIP IMS trunks to coexist on
               the same server with stations that dont always use SIP IMS trunks.
In other words, ELC is changing a previous marketing rule that
             the full-call model (CM-ES) and the half-call model (CM-FS) functions
can't co-exist on the same server.  As noted above, that also
                has the side effect that features which work differently under the
half-call model than under the full-call model now also can work
                differently for two different SIP stations on the same CM
server.
                 -->
             <xs:element name="extendedLocalCalls" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                    Only administrable if Hospitality is enabled on the System
Parameters
                 Customer-Options (Optional Features) screen. This field affects the
                    telephone display on calls that originated from a station with
Client
                    Room Class of Service. Note: For stations with an audix station
                    type, AUDIX Voice Power ports, or ports for any other type of
                    messaging that needs display information, Display Client
Redirection
```

```
                    must be enabled.
                    Set true to redirect information for a call originating from a
Client Room and terminating to this station displays.
                -->
                <xs:element name="displayClientRedirection" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    Valid Entries         Usage
                        true            Indicates that a station's line selection
is not to be moved from the currently selected line button
                                        to a different, non-alerting line button.
If you enter true, the line selection on an on-hook station only moves from the last
                                        used line button to a line button with an
audibly alerting call. If there are no alerting calls, the line selection
                                        remains on the button last used for a call.
                        false            The line selection on an on-hook station
with no alerting calls can be moved to a different line button, which might be
serving a different
                                        extension.
                 -->
                <xs:element name="selectLastUsedAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!-- Whether an unanswered forwarded call is provided coverage
treatment. -->
                <xs:element name="coverageAfterForwarding" type="xs:string"
maxOccurs="1" minOccurs="0" />

              <!-- Allow/disallow direct audio connections between IP endpoints. -->
                <xs:element name="directIpIpAudioConnections" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!-- Allows IP endpoints to be connected through the server's IP
circuit pack. -->
               <xs:element name="ipAudioHairpinning" type="xs:boolean" maxOccurs="1"
minOccurs="0" />


                <xs:element name="primeAppearancePreference" type="xs:string"
maxOccurs="1" minOccurs="0" />

                <!-- Elements with complex data type. Please refer the appropriate
elements for more details. -->
                <xs:element name="stationSiteData" type="csm:xmlStationSiteData"
maxOccurs="1" minOccurs="0" />
                <xs:element name="abbrList"
type="csm:xmlStationAbbreviatedDialingData" maxOccurs="unbounded" minOccurs="0" />
                <xs:element name="buttons" type="csm:xmlButtonData" maxOccurs="24"
minOccurs="0" />
                <xs:element name="featureButtons" type="csm:xmlButtonData"
maxOccurs="24" minOccurs="0" />
                <xs:element name="expansionModuleButtons" type="csm:xmlButtonData"
maxOccurs="72" minOccurs="0" />
                 <xs:element name="softKeys" type="csm:xmlButtonData" maxOccurs="15"
minOccurs="0" />
                <xs:element name="displayButtons" type="csm:xmlButtonData"
maxOccurs="unbounded" minOccurs="0" />
               <xs:element name="stationDataModule" type="csm:xmlStationDataModule"
maxOccurs="1" minOccurs="0" />
                <xs:element name="hotLineData" type="csm:xmlStationHotLineData"
maxOccurs="1" minOccurs="0" />
                <xs:element  name="nativeName" type="csm:xmlNativeNameData"
maxOccurs="1" minOccurs="0"/>
```

```
                <!-- Number of button modules -->
                <xs:element name="buttonModules" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:int">
                            <xs:minInclusive value="0" />
                            <xs:maxInclusive value="3" />
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <xs:element name="unconditionalInternalDest" maxOccurs="1"
minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <xs:element name="unconditionalInternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <xs:element name="unconditionalExternalDest" maxOccurs="1"
minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <xs:element name="unconditionalExternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <xs:element name="busyInternalDest" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

              <xs:element name="busyInternalActive" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="busyExternalDest" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

              <xs:element name="busyExternalActive" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

               <xs:element name="noReplyInternalDest" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
```

```
                        <xs:restriction base="xs:string">
                          <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="noReplyInternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

               <xs:element name="noReplyExternalDest" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="noReplyExternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <xs:element name="sacCfOverride" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="a"/>
                            <xs:enumeration value="n"/>
                            <xs:enumeration value="y"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="lossGroup" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:int">
                            <xs:minInclusive value="1" />
                            <xs:maxInclusive value="19" />
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="timeOfDayLockTable" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:int">
                            <xs:minInclusive value="1" />
                            <xs:maxInclusive value="5" />
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="emuLoginAllowed" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="ec500State" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="enabled"/>
                            <xs:enumeration value="disabled"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

               <!-- true/false to enable/disable Mute on Off Hook in Shared Control
Mode feature. -->
                <xs:element name="muteOnOffHookInSCMode" type="xs:boolean"
```

```
maxOccurs="1" minOccurs="0" />

                <xs:element name="type3pccEnabled" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="None"/>
                            <xs:enumeration value="Avaya"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="sipTrunk" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                           <xs:pattern value="aar|ars|[1-9]|[1-9][0-9]|[1-9]([0-9])
{2}|[1]([0-9]){3}|2000"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="multimediaEarlyAnswer" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="bridgedApprOrigRestr" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <xs:element name="callApprDispFormat" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="inter-location"/>
                            <xs:enumeration value="intra-location"/>
                            <xs:enumeration value="disp-param-default"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="ipPhoneGroupId" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:int">
                            <xs:minInclusive value="0" />
                            <xs:maxInclusive value="999" />
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="xoipEndPointType" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="auto"/>
                            <xs:enumeration value="fax"/>
                            <xs:enumeration value="modem"/>
                            <xs:enumeration value="tty"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

               <xs:element name="xid" type="xs:boolean" maxOccurs="1" minOccurs="0" /
>
                <xs:element name="stepClearing" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="fixedTei" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="tei" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
```

```
                            <xs:pattern value="[0-6][0-3]"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="countryProtocol" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="1"/>
                          <xs:enumeration value="2"/>
                          <xs:enumeration value="3"/>
                          <xs:enumeration value="6"/>
                          <xs:enumeration value="etsi"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="endptInit" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="spid" maxOccurs="1" minOccurs="0"  >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{1,10}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>


               <xs:element name="endptId" maxOccurs="1" minOccurs="0" > <!-- 00 to
62 -->
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:pattern value="[0-6][0-2]"/>
                       </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="isMCTSignalling" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="isShortCallingPartyDisplay" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="passageWay" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="dtmfOverIp" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="in-band"/>
                          <xs:enumeration value="in-band-g711"/>
                          <xs:enumeration value="out-of-band"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
                <xs:element name="location" type="xs:string" maxOccurs="1"
minOccurs="0" />
            </xs:sequence>
        </xs:extension>
   </xs:complexContent>
</xs:complexType>


<xs:complexType name="xmlStationSiteData">
    <xs:sequence>
        <xs:element name="room" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
```

```
                <xs:restriction base="xs:string">
                  <xs:maxLength value="10"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="jack" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:maxLength value="5"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="cable" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:maxLength value="5"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="floor" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="building" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="headset" type="xs:boolean" maxOccurs="1" minOccurs="0" />
        <xs:element name="speaker" type="xs:boolean" maxOccurs="1" minOccurs="0" />

        <xs:element name="mounting" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="d"/>
                  <xs:enumeration value="w"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="cordLength" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:int">
                  <xs:minInclusive value="0" />
                  <xs:maxInclusive value="99" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="setColor" type="xs:string" maxOccurs="1" minOccurs="0" />
    </xs:sequence>
</xs:complexType>


<xs:complexType name="xmlStationAbbreviatedDialingData">
    <xs:sequence>
        <xs:element name="listType" maxOccurs="1" minOccurs="1" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="enhanced"/>
                  <xs:enumeration value="group"/>
                  <xs:enumeration value="personal"/>
                  <xs:enumeration value="system"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="number" type="xs:int" maxOccurs="1" minOccurs="1" />
    </xs:sequence>
</xs:complexType>
```

```
<xs:complexType name="xmlButtonData">
    <xs:sequence>
        <xs:element name="number" type="xs:int" maxOccurs="1" minOccurs="1" /><!--
*******Must present******  -->
       <xs:element name="type" type="xs:string" maxOccurs="1" minOccurs="1" /><!--
*******Must present******  -->
        <xs:element name="data1" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="data2" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="data3" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="data4" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="data5" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="data6" type="xs:string" maxOccurs="1" minOccurs="0" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlStationDataModule">
    <xs:sequence>
        <xs:element name="dataExtension" maxOccurs="1" minOccurs="1" ><!--
*******Must present******  -->
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="[0-9]+([.-][0-9]+)*"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="name" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="29"/>

                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="cor" maxOccurs="1" minOccurs="1" ><!--  *******Must
present******  -->
            <xs:simpleType>
                  <xs:restriction base="xs:int">
                    <xs:minInclusive value="0" />
                    <xs:maxInclusive value="995" />
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="cos" maxOccurs="1" minOccurs="1" ><!--  *******Must
present******  -->
            <xs:simpleType>
                  <xs:restriction base="xs:int">
                    <xs:minInclusive value="0" />
                    <xs:maxInclusive value="15" />
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="itc" maxOccurs="1" minOccurs="1" ><!--  *******Must
present******  -->
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="restricted"/>
                    <xs:enumeration value="unrestricted"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="tn" maxOccurs="1" minOccurs="1" ><!--  *******Must
present******  -->
```

```
            <xs:simpleType>
                  <xs:restriction base="xs:int">
                    <xs:minInclusive value="0" />
                    <xs:maxInclusive value="100" />
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="listType" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="enhanced"/>
                    <xs:enumeration value="group"/>
                    <xs:enumeration value="personal"/>
                    <xs:enumeration value="system"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="listId" type="xs:int" maxOccurs="1" minOccurs="0" />

        <xs:element name="specialDialingOption" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="default"/>
                    <xs:enumeration value="hot-line"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="specialDialingAbbrDialCode" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="4"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlStationHotLineData">
    <xs:sequence>
        <xs:element name="hotLineDestAbbrevList" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:int">
                    <xs:minInclusive value="1" />
                    <xs:maxInclusive value="3" />
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="hotLineAbbrevDialCode" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]*"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
    </xs:sequence>
</xs:complexType>
<   Please find below locale for multiscript language
       Language              Locale
       Japanese                   ja
       Simplified Chinese        zh-cn
       Traditional Chinese     zh-tw
       Korean                       ko-kr
       Vietnamese                   vi-vn-->
<xs:complexType name="xmlNativeNameData">
    <xs:sequence>
```

```
        <xs:element name="locale" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="name" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="27"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>

</xs:schema>
```

Sample XML for bulk import of endpoint profiles

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
    <tns:user>
        <authenticationType>BASIC</authenticationType>
        <description>description</description>
        <displayName>displayname</displayName>
        <displayNameAscii>displayNameAscii</displayNameAscii>
        <dn>dn</dn>
        <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>givenName00</givenName>
        <honorific>honorific</honorific>
        <loginName>user00_00xyz@avaya.com</loginName>
        <middleName>middleName</middleName>
        <managerName>managerName</managerName>
        <preferredGivenName>preferredGivenName</preferredGivenName>
        <preferredLanguage>preferredLanguage</preferredLanguage>
        <source>local</source>
        <sourceUserKey>sourceUserKey</sourceUserKey>
        <status>AUTHPENDING</status>
        <suffix>suffix</suffix>
        <surname>surname</surname>
        <timeZone>timeZone</timeZone>
        <title>title</title>
        <userName>userName00</userName>
        <userPassword>userPassword</userPassword>
        <commPassword>commPassword</commPassword>
        <userType>ADMINISTRATOR</userType>
        <commProfileSet>
            <commProfileSetName>
                commProfileSetName00
            </commProfileSetName>
            <isPrimary>true</isPrimary>
            <commProfileList>
                <commProfile xsi:type="ipt:xmlStationProfile"
                    xmlns:ipt="http://xml.avaya.com/schema/import_csm_cm">
                    <commProfileType>CM</commProfileType>
                    <ipt:cmName>PUIM81</ipt:cmName>
                    <ipt:useExistingExtension>
                        false
                    </ipt:useExistingExtension>
                    <ipt:extension>7100000</ipt:extension>
                    <ipt:template>DEFAULT_4620_CM_6_0</ipt:template>
                    <ipt:setType>4620</ipt:setType>
                    <ipt:securityCode>78974231</ipt:securityCode>
                    <ipt:port>IP</ipt:port>
                    <ipt:coveragePath1>1</ipt:coveragePath1>
```

```
                    <ipt:tn>1</ipt:tn>
                    <ipt:cor>10</ipt:cor>
                    <ipt:cos>4</ipt:cos>
                    <ipt:dataModule>false</ipt:dataModule>
                    <ipt:speakerphone>1-way</ipt:speakerphone>
                    <ipt:displayLanguage>english</ipt:displayLanguage>
                    <ipt:ipSoftphone>false</ipt:ipSoftphone>
                    <ipt:survivableCOR>internal</ipt:survivableCOR>
                    <ipt:survivableTrunkDest>
                        true
                    </ipt:survivableTrunkDest>
                    <ipt:offPremisesStation>
                        false
                    </ipt:offPremisesStation>
                    <ipt:dataOption>none</ipt:dataOption>
                    <ipt:displayModule>false</ipt:displayModule>
                    <ipt:lwcReception>spe</ipt:lwcReception>
                    <ipt:lwcActivation>true</ipt:lwcActivation>
                    <ipt:lwcLogExternalCalls>
                        false
                    </ipt:lwcLogExternalCalls>
                    <ipt:cdrPrivacy>false</ipt:cdrPrivacy>
                    <ipt:redirectNotification>
                        true
                    </ipt:redirectNotification>
                    <ipt:perButtonRingControl>
                        false
                    </ipt:perButtonRingControl>
                    <ipt:bridgedCallAlerting>
                        false
                    </ipt:bridgedCallAlerting>
                    <ipt:bridgedIdleLinePreference>
                        false
                    </ipt:bridgedIdleLinePreference>
                    <!-- <ipt:confTransOnPrimaryAppearance></
ipt:confTransOnPrimaryAppearance>
                        <ipt:customizableLabels></ipt:customizableLabels> -->
                    <ipt:expansionModule>true</ipt:expansionModule>
                    <ipt:ipVideoSoftphone>false</ipt:ipVideoSoftphone>
                    <ipt:activeStationRinging>
                        single
                    </ipt:activeStationRinging>
                    <!-- <ipt:idleActiveRinging></ipt:idleActiveRinging>
                        <ipt:switchhookFlash></ipt:switchhookFlash>
                        <ipt:ignoreRotaryDigits></ipt:ignoreRotaryDigits>-->
                    <ipt:h320Conversion>false</ipt:h320Conversion>
                    <ipt:serviceLinkMode>as-needed</ipt:serviceLinkMode>
                    <ipt:multimediaMode>enhanced</ipt:multimediaMode>
                    <!-- <ipt:mwiServedUserType></ipt:mwiServedUserType>  -->
                    <!-- <ipt:audixName></ipt:audixName>  -->
                    <!-- <ipt:automaticMoves></ipt:automaticMoves>  -->
                    <ipt:remoteSoftphoneEmergencyCalls>
                        as-on-local
                    </ipt:remoteSoftphoneEmergencyCalls>
                    <!-- <ipt:alwaysUse></ipt:alwaysUse>  -->
                    <ipt:precedenceCallWaiting>
                        false
                    </ipt:precedenceCallWaiting>
                    <ipt:autoSelectAnyIdleAppearance>
                        false
                    </ipt:autoSelectAnyIdleAppearance>
                    <ipt:coverageMsgRetrieval>
                        true
                    </ipt:coverageMsgRetrieval>
                    <ipt:autoAnswer>none</ipt:autoAnswer>
```

```
                    <ipt:dataRestriction>false</ipt:dataRestriction>
                    <ipt:idleAppearancePreference>
                        false
                    </ipt:idleAppearancePreference>
                    <!-- <ipt:attCallWaitingIndication></
ipt:attCallWaitingIndication>  -->
                <!-- <ipt:distinctiveAudibleAlert></ipt:distinctiveAudibleAlert>
-->
                    <ipt:restrictLastAppearance>
                        true
                    </ipt:restrictLastAppearance>
                    <!-- <ipt:adjunctSupervision></ipt:adjunctSupervision>  -->
                    <!-- <ipt:perStationCpnSendCallingNumber></
ipt:perStationCpnSendCallingNumber>  -->
                    <!-- <ipt:busyAutoCallbackWithoutFlash></
ipt:busyAutoCallbackWithoutFlash>  -->
                    <ipt:audibleMessageWaiting>
                        false
                    </ipt:audibleMessageWaiting>
                    <ipt:displayClientRedirection>
                        false
                    </ipt:displayClientRedirection>
                    <ipt:selectLastUsedAppearance>
                        false
                    </ipt:selectLastUsedAppearance>
                    <ipt:coverageAfterForwarding>
                        s
                    </ipt:coverageAfterForwarding>
                    <ipt:directIpIpAudioConnections>
                        true
                    </ipt:directIpIpAudioConnections>
                    <ipt:ipAudioHairpinning>
                        false
                    </ipt:ipAudioHairpinning>
                    <!-- <ipt:primeAppearancePreference></
ipt:primeAppearancePreference>  -->
                </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of messaging profiles

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:one="http://xml.avaya.com/schema/import" elementFormDefault="qualified"
    targetNamespace="http://xml.avaya.com/schema/import_csm_mm" xmlns:csm="http://
xml.avaya.com/schema/import_csm_mm">

    <xs:import namespace="http://xml.avaya.com/schema/import"
        schemaLocation="userimport.xsd" />
    <!--Changes in xsd file need to generate jaxb src using this xsd-->
    <xs:complexType name="xmlMessagingProfile">
        <xs:complexContent>
            <xs:extension base="one:xmlCommProfileType">
                <xs:sequence>
                    <!--
                        Specifies the messaging system of the subscriber you want
to add.
                        Name as it appears under 'Applications/Application
                        Management/Entities
                    -->
                    <xs:element name="messagingName" type="xs:string"
                        maxOccurs="1" minOccurs="1" />
```

```
                    <xs:element name="useExisting" type="xs:boolean"
                        maxOccurs="1" minOccurs="0" /><!-- use existing -->

                    <!-- Specifies the messaging template of a subscriber.  -->
                    <xs:element name="messagingTemplate" type="xs:string"
                        maxOccurs="1" minOccurs="0" />


                    <xs:element name="mailboxNumber" maxOccurs="1"
                        minOccurs="1">
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[0-9]{1,50}" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>

                    <!--
                     Specifies the default password the subscriber must use to log in
                        to his or her mailbox. The password can be from one digit in
                        length to a maximum of 15 digits.
                    -->
                    <xs:element name="password" maxOccurs="1" minOccurs="0">
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[0-9]{0,15}" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>
                    <xs:element name="deleteOnUnassign" type="xs:boolean"
                        maxOccurs="1" minOccurs="0" />

                    <!-- follows overrriding  subscriber  data  -->

                    <!--
                        The class of service for this subscriber. The COS controls
                        subscriber access to many features and provides general
settings,
                        such as mailbox size.
                    -->
                   <xs:element name="cos" maxOccurs="1" minOccurs="0"> <!-- MM/CMM
field -->
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern
                                 value="[0-9]|[0-9]{2}|[0-4][0-9]{2}|[5][0-4][0-9]|
[5][5][0-1]" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>

                    <!--
                     Specifies the default community ID for the subscriber. Community
                        IDs are used to control message sending and receiving among
groups
                        of subscribers. The default value is 1.
                    -->
                  <xs:element name="communityID" maxOccurs="1" minOccurs="0"> <!--
MM/CMM field -->
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[0-9]|[0-1][0-5]" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>
```

```
                    <!--
                        Specifies the name that appears before the machine name and
domain
                     in the subscriber's e-mail address. The machine name and domain
                        are automatically added to the handle you enter when the
                        subscriber sends or receives an e-mail.
                    -->
                   <xs:element name="emailHandle" maxOccurs="1" minOccurs="0"> <!--
MM/CMM field -->
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="^[a-zA-Z0-9\w\.\-]*" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>

                    <!--
                        Specifies the display name of the subscriber in address book
                     listings, such as those for e-mail client applications. The name
                        you enter can be 1 to 64 characters in length.
                    -->
                    <xs:element name="commonName" type="xs:string"
                        maxOccurs="1" minOccurs="0" /> <!-- MM/CMM field -->

                    <!--
                      Specifies one or more alternate number to reach a subscriber.
You
                      can use secondary extensions to specify a telephone number for
                      direct reception of faxes, to allow callers to use an existing
                      Caller Application, or to identify each line appearance on the
                        subscriber's telephone set if they have different telephone
                        numbers.
                    -->
                    <xs:element name="secondaryExtension" maxOccurs="1"
                        minOccurs="0"> <!-- MM/CMM field -->
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[0-9]{0,50}" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>

                    <xs:element name="mmSpecific" type="csm:xmlMMSpecific"
                        maxOccurs="1" minOccurs="0" />
                    <xs:element name="cmmSpecific" type="csm:xmlCMMSpecific"
                        maxOccurs="1" minOccurs="0" />
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>


    <xs:complexType name="xmlMMSpecific">
        <xs:sequence>
            <!--
                Specifies a unique address in the voice mail network. The numeric
                address can be from 1 to 50 digits and can contain the Mailbox
                Number.
            -->
            <xs:element name="numericAddress" maxOccurs="1" minOccurs="0"> <!-- MM
field -->
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:pattern value="([0-9])*" />
```

```
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>

            <!-- The primary telephone extension of the subscriber. -->
            <xs:element name="pbxExtension" maxOccurs="1" minOccurs="0"> <!-- MM
field -->
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:pattern value="([+0-9])*" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>

            <!--
                The telephone number of the subscriber as displayed in address book
                listings and client applications. The entry can be a maximum of 50
                characters in length and can contain any combination of digits
                (0-9), period (.), hyphen (-), plus sign (+), and left and right
                parentheses ([) and (]).
            -->
            <xs:element name="telephoneNumber" maxOccurs="1"
                minOccurs="0"> <!-- MM field -->
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:pattern value="([-+\.()0-9])*" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>

            <!--
                If the subscriber name is entered in multi-byte character format,
                then this field specifies the ASCII translation of the subscriber
                name.
            -->
            <xs:element name="asciiVersionOfName" type="xs:string"
                maxOccurs="1" minOccurs="0" /> <!-- MM field -->

            <!--
                Specifies whether your password expires or not. You can choose one
                of the following: - yes: for password to expire - no: if you do not
                want your password to expire
            -->
            <xs:element name="expirePassword" type="csm:xmlyesNoType"
                maxOccurs="1" minOccurs="0" />  <!-- MM field -->

            <!--
                Specifies whether you want your mailbox to be locked. A subscriber
                mailbox can become locked after two unsuccessful login attempts. You
                can choose one of the following: - no: to unlock your mailbox - yes:
                to lock your mailbox and prevent access to it
            -->
            <xs:element name="mailBoxLocked" type="csm:xmlyesNoType"
                maxOccurs="1" minOccurs="0" />  <!-- MM field -->

            <!--
                Specifies the mailbox number or transfer dial string of the
                subscriber's personal operator or assistant. This field also
                indicates the transfer target when a caller to this subscriber
                presses 0 while listening to the subscriber's greeting.
            -->
            <xs:element name="personalOperatorMailbox" maxOccurs="1"
                minOccurs="0"> <!-- MM field -->
                <xs:simpleType>
                    <xs:restriction base="xs:string">
```

```
                    <xs:pattern value="[0-9]+([*#,][0-9]+)*" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            Specifies when to route calls to the backup operator mailbox. The
            default value for this field is Always Active.
        -->
        <xs:element name="personalOperatorSchedule" type="xs:string"
            maxOccurs="1" minOccurs="0" /> <!-- MM field -->

        <!--
            Specifies the order in which the subscriber hears the voice
            messages. You can choose one of the following: - urgent first then
            newest: to direct the system to play any messages marked as urgent
            prior to playing non-urgent messages. Both the urgent and non-urgent
            messages are played in the reverse order of how they were received.
            - oldest messages first: to direct the system to play messages in
            the order they were received. - urgent first then oldest: to direct
            the system to play any messages marked as urgent prior to playing
            non-urgent messages. Both the urgent and non-urgent messages are
            played in the order of how they were received. - newest messages
            first: to direct the system to play messages in the reverse order of
            how they were received.
        -->
        <xs:element name="tuiMessageOrder" maxOccurs="1"
            minOccurs="0"> <!-- MM field -->
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="urgent first then newest" />
                    <xs:enumeration value="oldest messages first" />
                    <xs:enumeration value="newest messages first" />
                    <xs:enumeration value="urgent first then oldest" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            Specifies the intercom paging settings for a subscriber. You can
            choose one of the following: - paging is off: to disable intercom
            paging for this subscriber. - paging is manual: if the subscriber
            can modify, with Subscriber Options or the TUI, the setting that
            allows callers to page the subscriber. - paging is automatic: if the
            TUI automatically allows callers to page the subscriber.
        -->
        <xs:element name="intercomPaging" maxOccurs="1" minOccurs="0"> <!-- MM
field -->
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="paging is off" />
                    <xs:enumeration value="paging is manual" />
                    <xs:enumeration value="paging is automatic" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            Specifies whether a subscriber can receive messages, e-mail messages
            and call-answer messages from other subscribers. You can choose one
            of the following: - yes: to allow the subscriber to create, forward,
            and receive messages. - no: to prevent the subscriber from receiving
            call-answer messages and to hide the subscriber from the telephone
            user interface (TUI). The subscriber cannot use the TUI to access
            the mailbox, and other TUI users cannot address messages to the
```

```
                subscriber.
            -->
            <xs:element name="voiceMailEnabled" type="csm:xmlTrueFalseType"
                maxOccurs="1" minOccurs="0" />

            <!--
                Specifies additional, useful information about a subscriber. Entries
                in this field are for convenience and are not used by the messaging
                system.
            -->
            <xs:element name="miscellaneous1" type="csm:xmlLength51Type"
                maxOccurs="1" minOccurs="0" />

            <!--
                Specifies additional, useful information about a subscriber. Entries
                in this field are for convenience and are not used by the messaging
                system.
            -->
            <xs:element name="miscellaneous2" type="csm:xmlLength51Type"
                maxOccurs="1" minOccurs="0" />

            <!--
                Specifies additional, useful information about a subscriber. Entries
                in this field are for convenience and are not used by the messaging
                system.
            -->
            <xs:element name="miscellaneous3" type="csm:xmlLength51Type"
                maxOccurs="1" minOccurs="0" />

            <!--
                Specifies additional, useful information about a subscriber. Entries
                in this field are for convenience and are not used by the messaging
                system.
            -->
            <xs:element name="miscellaneous4" type="csm:xmlLength51Type"
                maxOccurs="1" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlCMMSpecific">
        <xs:sequence>

            <!--
                Specifies the number of the switch on which this subscriber's
                extension is administered. You can enter "0" through "99", or leave
                this field blank. - Leave this field blank if the host switch number
                should be used. - Enter a "0" if no message waiting indicators
                should be sent for this subscriber. You should enter 0 when the
                subscriber does not have a phone on any switch in the network.
            -->
            <xs:element name="switchNumber" maxOccurs="1" minOccurs="0"> <!-- CMM
field -->
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:pattern value="[0-9]|[0-9][0-9]" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>

            <!--
                Specifies the Subscriber Account Code. The Subscriber Account Code
                is used to create Call Detail Records on the switch for calls placed
                by the voice ports. The value you enter in this field can contain
                any combination of digits from 0 to 9. If an account code is not
                specified, the system will use the subscriber's mailbox extension as
```

```
                the account code.
            -->
            <xs:element name="accountCode" maxOccurs="1" minOccurs="0"> <!-- CMM
field -->
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:pattern value="([0-9])*" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>

            <!--
                Specifies the number to be used as the default destination for the
                Transfer Out of Messaging feature. You can enter 3 to 10 digits in
                this field depending on the length of the system's extension, or
                leave this field blank.
            -->
            <xs:element name="coveringExtension" maxOccurs="1"
                minOccurs="0"> <!-- CMM field -->
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:pattern value="[0-9]{0}|[0-9]{3,10}" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>

            <!--
                Specifies additional, useful information about a subscriber. Entries
                in this field are for convenience and are not used by the messaging
                system.
            -->
            <xs:element name="miscellaneous1" type="csm:xmlLength11Type"
                maxOccurs="1" minOccurs="0" />

            <!--
                Specifies additional, useful information about a subscriber. Entries
                in this field are for convenience and are not used by the messaging
                system.
            -->
            <xs:element name="miscellaneous2" type="csm:xmlLength11Type"
                maxOccurs="1" minOccurs="0" />

            <!--
                Specifies additional, useful information about a subscriber. Entries
                in this field are for convenience and are not used by the messaging
                system.
            -->
            <xs:element name="miscellaneous3" type="csm:xmlLength11Type"
                maxOccurs="1" minOccurs="0" />

            <!--
                Specifies additional, useful information about a subscriber. Entries
                in this field are for convenience and are not used by the messaging
                system.
            -->
            <xs:element name="miscellaneous4" type="csm:xmlLength11Type"
                maxOccurs="1" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>

    <xs:simpleType name="xmlyesNoType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="Yes" />
            <xs:enumeration value="No" />
        </xs:restriction>
```

```
    </xs:simpleType>

    <xs:simpleType name="xmlTrueFalseType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="TRUE" />
            <xs:enumeration value="FALSE" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="xmlLength11Type">
        <xs:restriction base="xs:string">
            <xs:maxLength value="11" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="xmlLength51Type">
        <xs:restriction base="xs:string">
            <xs:maxLength value="51" />
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

Sample XML for bulk import of messaging profiles

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
    <tns:user>
        <authenticationType>BASIC</authenticationType>
        <description>description</description>
        <displayName>displayname</displayName>
        <displayNameAscii>displayNameAscii</displayNameAscii>
        <dn>dn</dn>
        <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>givenName00</givenName>
        <honorific>honorific</honorific>
        <loginName>user00_00xyz@avaya.com</loginName>
        <middleName>middleName</middleName>
        <managerName>managerName</managerName>
        <preferredGivenName>preferredGivenName</preferredGivenName>
        <preferredLanguage>preferredLanguage</preferredLanguage>
        <source>local</source>
        <sourceUserKey>sourceUserKey</sourceUserKey>
        <status>AUTHPENDING</status>
        <suffix>suffix</suffix>
        <surname>surname</surname>
        <timeZone>timeZone</timeZone>
        <title>title</title>
        <userName>userName00</userName>
        <userPassword>userPassword</userPassword>
        <commPassword>commPassword</commPassword>
        <userType>ADMINISTRATOR</userType>
        <commProfileSet>
            <commProfileSetName>
                commProfileSetName00
            </commProfileSetName>
            <isPrimary>true</isPrimary>
            <commProfileList>
                <commProfile xsi:type="ipt:xmlMessagingProfile"
                    xmlns:ipt="http://xml.avaya.com/schema/import_csm_mm">
                    <commProfileType>Messaging</commProfileType>
                    <ipt:messagingName>MM-155-187</ipt:messagingName>
```

```
                    <ipt:useExisting>false</ipt:useExisting>
                    <ipt:messagingTemplate>
                        DEFAULT_MM_5_2
                    </ipt:messagingTemplate>
                    <ipt:mailboxNumber>3201</ipt:mailboxNumber>
                    <ipt:password>534456346</ipt:password>
                    <ipt:cos>0</ipt:cos>
                    <ipt:communityID>1</ipt:communityID>
                    <ipt:mmSpecific>
                        <ipt:numericAddress>3201</ipt:numericAddress>
                        <ipt:pbxExtension>32134</ipt:pbxExtension>
                        <ipt:telephoneNumber>42342</ipt:telephoneNumber>
                        <!--<ipt:expirePassword></ipt:expirePassword>-->
                        <ipt:tuiMessageOrder>newest messages first
</ipt:tuiMessageOrder>
                        <ipt:intercomPaging>paging is off
</ipt:intercomPaging>
                        <ipt:voiceMailEnabled>
                            FALSE
                        </ipt:voiceMailEnabled>
                        <ipt:miscellaneous1>
                            Miscellaneous
                        </ipt:miscellaneous1>
                    </ipt:mmSpecific>
                </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of agent profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:one="http://
xml.avaya.com/schema/import" elementFormDefault="qualified"
targetNamespace="http://xml.avaya.com/schema/import_csm_agent" xmlns:csm="http://
xml.avaya.com/schema/import_csm_agent">
<xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>

<!--Changes in xsd file need to generate jaxb src using this xsd-->
<xs:complexType name="xmlAgentProfile">
    <xs:complexContent>
           <xs:extension base="one:xmlCommProfileType" >
            <xs:sequence>
              <!-- CM Name as it appears under 'Applications/Application Management/
Entities -->
               <xs:element name="cmName" type="xs:string" maxOccurs="1"
minOccurs="1"/>

               <!-- 'true' if already created extension is to be used.  'false' if
available extension is to be used. -->
               <xs:element name="useExistingAgent" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

              <!-- Agent Login ID extension number that need to be assigned to the
user. -->
               <xs:element name="loginIdExtension" maxOccurs="1" minOccurs="1">
                   <xs:simpleType>
                         <xs:restriction base="xs:string">
                           <xs:pattern value="[0-9]+([\.\-][0-9]+)*"/>
                       </xs:restriction>
                   </xs:simpleType>
               </xs:element>
```

```
                <!-- Template name to be used to create agent. Values defined in
Template will be used if not provided. -->
                <xs:element name="template" type="xs:string" maxOccurs="1"
minOccurs="0"/>

                <!-- Security code for station. Value can be digit only.  -->
                <xs:element name="securityCode" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{0,4}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

              <xs:element name="aas" type="xs:boolean" maxOccurs="1" minOccurs="0"/>
                <xs:element name="audix" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

                <xs:element name="password" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{0,9}" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="portExtension" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]+([\.\-][0-9]+)*"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Whether the agent should be deleted if it unassigned from the
user. -->
               <xs:element name="deleteOnUnassign" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

                <xs:element name="tn" maxOccurs="1" minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:int">
                            <xs:minInclusive value="0" />
                            <xs:maxInclusive value="100" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="cor" maxOccurs="1" minOccurs="0">
                      <xs:simpleType>
                        <xs:restriction base="xs:int">
                              <xs:minInclusive value="0"/>
                              <xs:maxInclusive value="995"/>
                        </xs:restriction>
                      </xs:simpleType>
                </xs:element>

                <xs:element name="coveragePath" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="(t[1-9][0-9]{0,2})|([1-9][0-9]{0,2}|
1[0-9]{3}|2000)"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
```

```
                <xs:element name="lwcReception" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="audix"/>
                            <xs:enumeration value="msa"/>
                            <xs:enumeration value="spe"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="lwcLogExternalCalls" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="audixNameforMessaging" type="xs:string"
maxOccurs="1" minOccurs="0" />
                <xs:element name="hearsServiceObservingTone" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="loginIDforISDNSIPDisplay" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <xs:element name="autoAnswer" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="acd"/>
                            <xs:enumeration value="all"/>
                            <xs:enumeration value="none"/>
                            <xs:enumeration value="station"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="miaAcrossSkills" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="n"/>
                            <xs:enumeration value="y"/>
                            <xs:enumeration value="system"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

              <xs:element name="acwAgentConsideredIdle" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="n"/>
                            <xs:enumeration value="y"/>
                            <xs:enumeration value="system"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

               <xs:element name="auxWorkReasonCodeType" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="forced"/>
                            <xs:enumeration value="requested"/>
                            <xs:enumeration value="system"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="logoutReasonCodeType" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
```

```
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="forced"/>
                          <xs:enumeration value="requested"/>
                          <xs:enumeration value="system"/>
                          <xs:enumeration value="none"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

              <xs:element name="maximumTimeAgentInAcwBeforeLogoutSec" maxOccurs="1"
minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="|[3-9][0-9]{1}|[1-9][0-9]{1,3}|
(none)|(system)"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="forcedAgentLogoutTimeHr" maxOccurs="1"
minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:pattern value="|[0-9]|[1][0-9]{1}|[2][0-3]{1}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="forcedAgentLogoutTimeSec" maxOccurs="1"
minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="|(00)|(15)|(30)|(45)"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="directAgentSkill" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:pattern value="|[1-9]|[1-9][0-9]{1}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

              <xs:element name="callHandlingPreference" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="greatest-need"/>
                          <xs:enumeration value="percent-allocation"/>
                          <xs:enumeration value="skill-level"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

               <xs:element name="serviceObjective" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="directAgentCallsFirst" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="localCallPreference" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <xs:element name="skills" type="csm:xmlAgentLoginIdSkillsData"
maxOccurs="unbounded" minOccurs="0" />
```

```
                <!--

                private String NativeNameScripts;

                 -->
            </xs:sequence>
        </xs:extension>
   </xs:complexContent>
</xs:complexType>

<xs:complexType name="xmlAgentLoginIdSkillsData">
    <xs:sequence>
    <!--
        private AgentLoginIdData agentLoginId;

     -->
        <xs:element name="number" type="xs:string" maxOccurs="1" minOccurs="1" />
        <xs:element name="skillNumber" maxOccurs="1" minOccurs="1">
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="|[1-9]|[1-9][0-9]{1}"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="reserveLevel" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="|[1-2]"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="skillLevel" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="|[1-9]|[1-9][0-6]{1}"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="percentAllocation" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="|[1-9]|[1-9][0-9]{1}|100"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>


    </xs:sequence>
</xs:complexType>


</xs:schema>
```

XML Schema for CS1000 and CallPilot Communication Profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:one="http://xml.avaya.com/schema/import"
     targetNamespace="http://xml.avaya.com/schema/import1"
     elementFormDefault="qualified"
     xmlns:abc="http://xml.avaya.com/schema/import1">
<xsd:import namespace="http://xml.avaya.com/schema/import"
```

```
            schemaLocation="userimport.xsd"/>
<xsd:complexType name="AccountCommProfileType">
    <xsd:complexContent>
        <xsd:extension base="one:xmlCommProfileType" >
            <xsd:sequence>
               <xsd:element name="serviceDetails" type="xsd:string" minOccurs="0"/>
               <xsd:element name="element" type="xsd:string" minOccurs="0"/>
               <xsd:element name="target" type="xsd:string" minOccurs="0"/>
               <xsd:element name="template" type="xsd:string" minOccurs="0"/>
               <xsd:element name="serviceType" type="xsd:string" minOccurs="0"/>
               <xsd:element name="accountDetails" type="xsd:string" minOccurs="0"/>
              <xsd:element name="accountProperties" type="abc:AccountPropertyType"
minOccurs="0" maxOccurs="unbounded"/>
            </xsd:sequence>
        </xsd:extension>
    </xsd:complexContent>
</xsd:complexType>

<xsd:complexType name="AccountPropertyType">
   <xsd:sequence>
      <xsd:element name="propertyName" type="xsd:string"/>
      <xsd:element name="propertyValue" type="xsd:string"/>
    </xsd:sequence>
</xsd:complexType>
</xsd:schema>
```

Sample XML for CS1000 and CallPilot Communication Profiles

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ns3="http://
xml.avaya.com/schema/import1" xmlns:ns4="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/import userimport.xsd">
    <tns:user>
        <authenticationType>basic</authenticationType>
        <description></description>
        <displayName>singleUser, singleUser</displayName>
        <displayNameAscii>singleUser, singleUser</displayNameAscii>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>singleUser</givenName>
        <honorific></honorific>
        <loginName>singleuser@avaya.com</loginName>
        <employeeNo></employeeNo>
        <department></department>
        <organization></organization>
        <middleName></middleName>
        <preferredLanguage>en_US</preferredLanguage>
        <source>local</source>
        <sourceUserKe>Ynone</sourceUserKe>Y
        <status>provisioned</status>
        <surname>singleUser</surname>
        <userName>singleuser</userName>
        <userPassword></userPassword>
        <roles>
            <role>End-User</role>
        </roles>
        <ownedContactLists>
            <contactList>
                <name>list-singleuser_avaya.com</name>
                <description></description>
                <isPublic>false</isPublic>
                <contactListType>general</contactListType>
            </contactList>
```

```
        </ownedContactLists>
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimar>Ytrue</isPrimar>Y
            <commProfileList>
               <commProfile xsi:type="ns3:AccountCommProfileType" xmlns:ns3="http://
xml.avaya.com/schema/import1">
                   <commProfileType>accountCommProfile</commProfileType>
                 <ns3:serviceDetails>DN=8054(Marped), TN=004 0 00 12, TYPE=M2602</
ns3:serviceDetails>
                   <ns3:element>CS1K Mock Element Manager</ns3:element>
                   <ns3:target>Target1</ns3:target>
                   <ns3:template>Premium</ns3:template>
<ns3:serviceType>com.nortel.ems.services.account.Telephony</ns3:serviceType>
                   <ns3:properties>
                       <ns3:property name="prefEsn">343-8054</ns3:propert>Y
                       <ns3:property name="prefDn">8054</ns3:propert>Y
                   </ns3:properties>
                   <ns3:isPublished>true</ns3:isPublished>
               </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema for Avaya Branch Gateway Communication Profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:one="http://xml.avaya.com/schema/import" elementFormDefault="qualified"
    targetNamespace="http://xml.avaya.com/schema/import_csm_b5800"
xmlns:csm="http://xml.avaya.com/schema/import_csm_b5800">

    <xs:import namespace="http://xml.avaya.com/schema/import"
        schemaLocation="userimport.xsd" />

    <!--Changes in xsd file need to generate jaxb src using this xsd-->
    <xs:complexType name="xmlB5800UserProfile">
        <xs:complexContent>
            <xs:extension base="one:xmlCommProfileType">
                <xs:sequence>
                    <!--
                        B5800/B5800L Device Name as it appears under 'Applications/
Application
                        Management/Entities
                    -->
                    <xs:element name="deviceName" type="xs:string" maxOccurs="1"
                        minOccurs="1" />

                    <!--
                       Template name to be used to create station. Values defined in
                        Template will be used if not provided.
                    -->
                    <xs:element name="userTemplate" type="xs:string"
                        maxOccurs="1" minOccurs="0" />

                    <xs:element name="useExistingExt" type="xs:boolean"
                        maxOccurs="1" minOccurs="0" />

                    <!-- extension number that need to be assigned to the user. -->
                    <xs:element name="extension" maxOccurs="1" minOccurs="1">
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[0-9]+([\.\-][0-9]+)*" />
                            </xs:restriction>
```

```
                    </xs:simpleType>
                </xs:element>

                <!-- Specifies the type of the extn  -->
                <xs:element name="extensionType" maxOccurs="1"
                    minOccurs="1">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:enumeration value="Analog" />
                            <xs:enumeration value="IPDECT" />
                            <xs:enumeration value="Sip" />
                            <xs:enumeration value="Digital" />
                            <xs:enumeration value="H323" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="deleteExtOnUserDelete" type="xs:boolean"
                    maxOccurs="1" minOccurs="0" />

                <xs:element name="data" type="csm:xmlB5800UserProfileData"
                    maxOccurs="1" minOccurs="0" />
            </xs:sequence>

        </xs:extension>

    </xs:complexContent>
</xs:complexType>

<xs:complexType name="xmlB5800UserProfileData">
    <xs:sequence>
        <xs:element name="ws_object" type="csm:xmlB5800UserConfig">
        </xs:element>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlB5800UserConfig">
    <xs:sequence>
        <xs:element name="Extension" type="csm:xmlB5800ExtensionInfo">
        </xs:element>
        <xs:element name="User" type="csm:xmlB5800UserInfo">
        </xs:element>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlB5800ExtensionInfo">
    <xs:sequence>
        <xs:element name="Id" type="xs:int" minOccurs="0" />
        <xs:element name="Extension" type="xs:string" minOccurs="0" />
        <xs:element name="TypeInfo" type="xs:int" minOccurs="0" />
        <xs:element name="CallerDisplayType" type="xs:int" minOccurs="0" />
        <xs:element name="MessageLampType" type="xs:int" minOccurs="0" />
        <xs:element name="ExtnClassification" type="xs:int" minOccurs="0" />
        <xs:element name="LineType" type="xs:int" minOccurs="0" />
        <xs:element name="MinFlashPulseWidth" type="xs:int" minOccurs="0" />
        <xs:element name="MaxFlashPulseWidth" type="xs:int" minOccurs="0" />
        <xs:element name="UseSystemFlashHook" type="xs:boolean" minOccurs="0" />
        <xs:element name="ResetVolumeAfterCalls" type="xs:boolean"
minOccurs="0" />
        <xs:element name="DisconnectPulseWidth" type="xs:int" minOccurs="0" />
        <xs:element name="HookPersistency" type="xs:int" minOccurs="0" />
        <xs:element name="Mac" type="xs:string" minOccurs="0" />
        <xs:element name="SilenceSuppression" type="xs:boolean" minOccurs="0" />
        <xs:element name="VoicePktSize" type="xs:int" minOccurs="0" />
        <xs:element name="VoiceCompression" type="xs:int" minOccurs="0" />
```

```
            <xs:element name="voip" type="csm:xmlVoip" minOccurs="0" />
            <xs:element name="RenegotiationSupported" type="xs:boolean"
minOccurs="0" />
            <xs:element name="RenegotiateBeforeConnect" type="xs:boolean"
minOccurs="0" />
            <xs:element name="UseVocoder" type="xs:boolean" minOccurs="0" />
           <xs:element name="EarlyH245Supported" type="xs:boolean" minOccurs="0" />
            <xs:element name="RFC2833" type="xs:boolean" minOccurs="0" />
            <xs:element name="MediaWait" type="xs:boolean" minOccurs="0" />
            <xs:element name="MediaOnOverlap" type="xs:boolean" minOccurs="0" />
            <xs:element name="PauseRequired" type="xs:boolean" minOccurs="0" />
           <xs:element name="PauseOnEndRequired" type="xs:boolean" minOccurs="0" />
            <xs:element name="ParallelH245" type="xs:boolean" minOccurs="0" />
            <xs:element name="AnnexFSupported" type="xs:boolean" minOccurs="0" />
            <xs:element name="PhoneType" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIAudio_setting" type="xs:int" minOccurs="0" />
           <xs:element name="ExtnAPIHeadset_setting" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIContrast" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIRedial_time" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPISpeaker_volume" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIHandsfree_settings" type="xs:int"
minOccurs="0" />
           <xs:element name="ExtnAPIRingtone_volume" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIDoor_phone" type="xs:boolean" minOccurs="0" />
            <xs:element name="ExtnAPIHandset_volume" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIRingtone_speed" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIHeadset_volume" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIHeadset_config" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIAlpha_keypad_layout" type="xs:int"
minOccurs="0" />
            <xs:element name="ExtnAPIDirect_dial_enabled" type="xs:boolean"
minOccurs="0" />
            <xs:element name="ExtnAPIHandsfree_enabled" type="xs:boolean"
minOccurs="0" />
            <xs:element name="T38Fax" type="csm:xmlT38Fax" minOccurs="0" />
            <xs:element name="SipExtn" type="csm:xmlSipExtn" minOccurs="0" />
            <xs:element name="DisableSpeaker" type="xs:boolean" minOccurs="0" />
            <xs:element name="VPNExtn" type="xs:boolean" minOccurs="0" />
            <xs:element name="IPAvayaLicenseReserved" type="xs:boolean"
minOccurs="0" />
            <xs:element name="IPEndpointsLicenseReserved" type="xs:boolean"
minOccurs="0" />
            <xs:element name="IsExtnCentralized" type="xs:boolean" minOccurs="0" />
          <xs:element name="CentralizedDDINumber" type="xs:string" minOccurs="0" />
            <xs:element name="ExtnDS" type="csm:xmlExtnDS" minOccurs="0" />
            <xs:element name="SpecificBstType" type="xs:int" minOccurs="0" />
        </xs:sequence>
        <xs:attribute name="GUID" type="xs:string" />
    </xs:complexType>

    <xs:complexType name="xmlB5800UserInfo">
        <xs:sequence>
            <xs:element name="UserRightsView" type="xs:string" minOccurs="0" />
            <xs:element name="UsingView" type="xs:boolean" minOccurs="0" />
          <xs:element name="UserRightsTimeProfile" type="xs:string" minOccurs="0" /
>
          <xs:element name="OutOfHoursUserRights" type="xs:string" minOccurs="0" />
            <xs:element name="Name" type="xs:string" minOccurs="0" />
            <xs:element name="KName" type="xs:string" minOccurs="0" />
            <xs:element name="Password" type="xs:string" minOccurs="0" />
            <xs:element name="FullName" type="xs:string" minOccurs="0" />
            <xs:element name="Extension" type="xs:string" minOccurs="0" />
            <xs:element name="Priority" type="xs:int" minOccurs="0" />
            <xs:element name="OutsideCallSeq" type="xs:int" minOccurs="0" />
            <xs:element name="InsideCallSeq" type="xs:int" minOccurs="0" />
```

```
            <xs:element name="RingbackCallSeq" type="xs:int" minOccurs="0" />
            <xs:element name="NoAnswerTime" type="xs:int" minOccurs="0" />
            <xs:element name="ForwardOnBusy" type="xs:boolean" minOccurs="0" />
           <xs:element name="BookConferenceWithPM" type="xs:boolean" minOccurs="0" /
>
           <xs:element name="DisableForwardOnInt" type="xs:boolean" minOccurs="0" />
            <xs:element name="DisableForwardUncondOnInt" type="xs:boolean"
minOccurs="0" />
            <xs:element name="DisableForwardBusyNoAnsOnInt" type="xs:boolean"
minOccurs="0" />
           <xs:element name="VoicemailReception2" type="xs:string" minOccurs="0" />
           <xs:element name="VoicemailReception3" type="xs:string" minOccurs="0" />
            <xs:element name="DSSKeys" type="csm:xmlDSSKeys" minOccurs="0" />
            <xs:element name="InhibitOffSwitchForwarding" type="xs:boolean"
minOccurs="0" />
            <xs:element name="IsNoUser" type="xs:boolean" minOccurs="0" />
            <xs:element name="IsRealUser" type="xs:boolean" minOccurs="0" />
            <xs:element name="IsRemoteManager" type="xs:boolean" minOccurs="0" />
            <xs:element name="IsVoiceEmailModeAlert" type="xs:boolean"
minOccurs="0" />
           <xs:element name="IsVoiceEmailModeCopy" type="xs:boolean" minOccurs="0" /
>
            <xs:element name="IsVoiceEmailModeForward" type="xs:boolean"
minOccurs="0" />
           <xs:element name="IsVoiceEmailModeOff" type="xs:boolean" minOccurs="0" />
            <xs:element name="MaxTwinnedCalls" type="xs:int" minOccurs="0" />
            <xs:element name="PhoneManagerCallStatusOptions" type="xs:long"
minOccurs="0" />
           <xs:element name="PhoneManagerCloseOptions" type="xs:int" minOccurs="0" /
>
            <xs:element name="PhoneManagerCanChange" type="xs:boolean"
minOccurs="0" />
            <xs:element name="PhoneManagerConfigureOptions" type="xs:int"
minOccurs="0" />
            <xs:element name="PhoneManagerOptions" type="xs:int" minOccurs="0" />
            <xs:element name="PhoneManagerOptionsOriginal" type="xs:int"
minOccurs="0" />
            <xs:element name="PhoneType" type="xs:int" minOccurs="0" />
            <xs:element name="PhoneTypeIndex" type="xs:int" minOccurs="0" />
            <xs:element name="PopupAnswering" type="xs:boolean" minOccurs="0" />
            <xs:element name="PopupExternal" type="xs:boolean" minOccurs="0" />
            <xs:element name="PopupInternal" type="xs:boolean" minOccurs="0" />
            <xs:element name="PopupOutlook" type="xs:boolean" minOccurs="0" />
            <xs:element name="PopupRinging" type="xs:boolean" minOccurs="0" />
            <xs:element name="PopupOptions" type="xs:int" minOccurs="0" />
            <xs:element maxOccurs="unbounded" name="RingDelay" type="xs:int"
minOccurs="0" />
            <xs:element name="ShowAccountCodes" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowAllCalls" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowCallStatus" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowCostOfCall" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowIncoming" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowMessages" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowMissed" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowOutgoing" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowSpeedDials" type="xs:boolean" minOccurs="0" />
           <xs:element name="StartInCompactMode" type="xs:boolean" minOccurs="0" />
            <xs:element name="StayInCompactModeOnIncommingCall" type="xs:boolean"
minOccurs="0" />
            <xs:element name="StayInCompaceModeOnOutgoingCall" type="xs:boolean"
minOccurs="0" />
           <xs:element name="T3AllowThirdPartyFwd" type="xs:boolean" minOccurs="0" /
>
            <xs:element name="T3ProtectFromThirdPartyFwd" type="xs:boolean"
minOccurs="0" />
```

```
            <xs:element name="TwinnedDialDelay" type="xs:int" minOccurs="0" />
            <xs:element name="TwinnedEligibleForForwarded" type="xs:boolean"
minOccurs="0" />
            <xs:element name="TwinnedEligibleForGroup" type="xs:boolean"
minOccurs="0" />
           <xs:element name="TwinnedMobileNumber" type="xs:string" minOccurs="0" />
            <xs:element name="TwinnedTimeProfile" type="xs:string" minOccurs="0" />
            <xs:element name="TwinningNumber" type="xs:string" minOccurs="0" />
            <xs:element name="TwinningType" type="xs:int" minOccurs="0" />
            <xs:element name="ForwardOnNoAnswer" type="xs:boolean" minOccurs="0" />
          <xs:element name="ForwardUnconditional" type="xs:boolean" minOccurs="0" /
>
            <xs:element name="ForwardHuntGroupCalls" type="xs:boolean"
minOccurs="0" />
            <xs:element name="ForwardNumber" type="xs:string" minOccurs="0" />
            <xs:element name="ForwardBusyNumber" type="xs:string" minOccurs="0" />
            <xs:element name="DoNotDisturb" type="xs:boolean" minOccurs="0" />
            <xs:element name="DNDExceptions" type="xs:string" minOccurs="0" />
            <xs:element name="OutgoingCallBar" type="xs:boolean" minOccurs="0" />
            <xs:element name="OffHookStation" type="xs:boolean" minOccurs="0" />
            <xs:element name="BusyOnHeld" type="xs:boolean" minOccurs="0" />
            <xs:element name="FollowMeNumber" type="xs:string" minOccurs="0" />
            <xs:element name="CallWaitingOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="VoicemailOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="VoicemailHelp" type="xs:boolean" minOccurs="0" />
            <xs:element name="VoicemailCode" type="xs:string" minOccurs="0" />
            <xs:element name="VoicemailEmail" type="xs:string" minOccurs="0" />
            <xs:element name="VoicemailEmailReading" type="xs:boolean"
minOccurs="0" />
            <xs:element name="VoicemailReception" type="xs:string" minOccurs="0" />
            <xs:element name="VoicemailEmailMode" type="xs:int" minOccurs="0" />
            <xs:element name="VoicemailRingback" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShortCodes" type="csm:xmlShortCodes" minOccurs="0" />
            <xs:element name="DialInOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="DialInTimeProfile" type="xs:string" minOccurs="0" />
          <xs:element name="DialInFirewallProfile" type="xs:string" minOccurs="0" /
>
            <xs:element name="SourceNumbers" type="xs:string" minOccurs="0" />
            <xs:element name="DialInQuotaTime" type="xs:int" minOccurs="0" />
            <xs:element name="LoginCode" type="xs:string" minOccurs="0" />
            <xs:element name="LoginIdleTime" type="xs:string" minOccurs="0" />
            <xs:element name="WrapUpTime" type="xs:int" minOccurs="0" />
            <xs:element name="TwinMaster" type="xs:string" minOccurs="0" />
           <xs:element name="SecTwinCallEnabled" type="xs:boolean" minOccurs="0" />
            <xs:element name="CanIntrude" type="xs:boolean" minOccurs="0" />
            <xs:element name="CannotBeIntruded" type="xs:boolean" minOccurs="0" />
            <xs:element name="XDirectory" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForceLogin" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForceAuthCode" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForceAccountCode" type="xs:boolean" minOccurs="0" />
            <xs:element name="SystemPhone" type="xs:int" minOccurs="0" />
            <xs:element name="AbsentMsg" type="xs:int" minOccurs="0" />
            <xs:element name="AbsentSet" type="xs:int" minOccurs="0" />
            <xs:element name="AbsentText" type="xs:string" minOccurs="0" />
            <xs:element name="T3HuntGroupMembershipStatus" type="xs:string"
minOccurs="0" />
            <xs:element name="T3HuntGroupServiceStatus" type="xs:string"
minOccurs="0" />
            <xs:element name="T3DirectoryEntries" type="xs:string" minOccurs="0" />
            <xs:element name="MonitorGroup" type="xs:string" minOccurs="0" />
            <xs:element name="DisplayLocale" type="xs:string" minOccurs="0" />
            <xs:element name="Locale" type="xs:string" minOccurs="0" />
            <xs:element name="PMType" type="xs:int" minOccurs="0" />
            <xs:element name="InboundAutoRecord" type="xs:int" minOccurs="0" />
            <xs:element name="OutboundAutoRecord" type="xs:int" minOccurs="0" />
```

```
          <xs:element name="AutoRecordTimeProfile" type="xs:string" minOccurs="0" /
>
           <xs:element name="RemoteWorker" type="xs:boolean" minOccurs="0" />
           <xs:element name="CanAcceptCollectCalls" type="xs:boolean"
minOccurs="0" />
           <xs:element name="UserRights" type="xs:string" minOccurs="0" />
           <xs:element name="Secretaries" type="xs:string" minOccurs="0" />
           <xs:element name="TransferReturnTime" type="xs:string" minOccurs="0" />
           <xs:element name="AnswerCallWaiting" type="xs:boolean" minOccurs="0" />
           <xs:element name="RingingLinePreference" type="xs:boolean"
minOccurs="0" />
          <xs:element name="IdleLinePreference" type="xs:boolean" minOccurs="0" />
           <xs:element name="CoverageTime" type="xs:int" minOccurs="0" />
           <xs:element name="AutoVRL" type="xs:int" minOccurs="0" />
           <xs:element name="ManualVRL" type="xs:int" minOccurs="0" />
           <xs:element name="DelayedRingPreference" type="xs:boolean"
minOccurs="0" />
           <xs:element name="AnswerPreSelect" type="xs:boolean" minOccurs="0" />
           <xs:element name="ReserveLastCA" type="xs:boolean" minOccurs="0" />
           <xs:element name="CallTracingOn" type="xs:boolean" minOccurs="0" />
           <xs:element name="DisplayCharges" type="xs:boolean" minOccurs="0" />
           <xs:element name="MarkUpFactor" type="xs:int" minOccurs="0" />
          <xs:element name="reset_longest_idle_info" type="xs:int" minOccurs="0" />
           <xs:element name="NoAnswerStatus" type="xs:int" minOccurs="0" />
           <xs:element name="PBXAddress" type="xs:string" minOccurs="0" />
           <xs:element name="SIPName" type="xs:string" minOccurs="0" />
           <xs:element name="SIPDisplayName" type="xs:string" minOccurs="0" />
           <xs:element name="SIPContact" type="xs:string" minOccurs="0" />
           <xs:element name="SIPAnonymous" type="xs:boolean" minOccurs="0" />
           <xs:element name="AbbreviatedRing" type="xs:boolean" minOccurs="0" />
          <xs:element name="CustomerServiceRep" type="xs:boolean" minOccurs="0" />
           <xs:element name="ACWTime" type="xs:int" minOccurs="0" />
           <xs:element name="AutoACW" type="xs:boolean" minOccurs="0" />
           <xs:element name="UMSWebServices" type="xs:boolean" minOccurs="0" />
           <xs:element name="DisableVMOnFU" type="xs:boolean" minOccurs="0" />
           <xs:element name="DTMFCallCtrl" type="xs:boolean" minOccurs="0" />
           <xs:element name="LoggedOutTwinning" type="xs:int" minOccurs="0" />
           <xs:element name="OneXClient" type="xs:boolean" minOccurs="0" />
           <xs:element name="MobilityFeatures" type="xs:boolean" minOccurs="0" />
           <xs:element name="TwinnedBridgeAppearances" type="xs:boolean"
minOccurs="0" />
           <xs:element name="TwinnedCoverageAppearances" type="xs:boolean"
minOccurs="0" />
           <xs:element name="TwinnedLineAppearances" type="xs:boolean"
minOccurs="0" />
           <xs:element name="PersonalDirectory" type="xs:string" minOccurs="0" />
          <xs:element name="ForwardToVoicemail" type="xs:boolean" minOccurs="0" />
           <xs:element name="CoverageGroup" type="xs:string" minOccurs="0" />
          <xs:element name="CanChangeHGOOSGroup" type="xs:string" minOccurs="0" />
           <xs:element name="CanChangeHGONGroup" type="xs:string" minOccurs="0" />
          <xs:element name="IncludeForwardInMenu" type="xs:boolean" minOccurs="0" /
>
           <xs:element name="CallLoggingCentralised" type="xs:string"
minOccurs="0" />
           <xs:element name="AttentionRing" type="xs:string" minOccurs="0" />
           <xs:element name="CoverageRing" type="xs:string" minOccurs="0" />
          <xs:element name="LogMissedCallsForHG" type="xs:string" minOccurs="0" />
           <xs:element name="DisableForwardToVoicemail" type="xs:int"
minOccurs="0" />
           <xs:element name="AnnouncementsOn" type="xs:boolean" minOccurs="0" />
           <xs:element name="FollowAnnouncementsOn" type="xs:boolean"
minOccurs="0" />
          <xs:element name="LoopAnnouncementsOn" type="xs:boolean" minOccurs="0" />
          <xs:element name="SyncAnnouncementsOn" type="xs:boolean" minOccurs="0" />
           <xs:element name="FirstAnnTime" type="xs:int" minOccurs="0" />
```

```
            <xs:element name="SecondAnnTime" type="xs:int" minOccurs="0" />
            <xs:element name="BetweenAnnTime" type="xs:int" minOccurs="0" />
            <xs:element name="PostAnnTone" type="xs:int" minOccurs="0" />
            <xs:element name="PortalServices" type="xs:int" minOccurs="0" />
            <xs:element name="WorkingHoursUserRightsGroup" type="xs:string"
minOccurs="0" />
            <xs:element name="T3SelfAdmin" type="xs:string" minOccurs="0" />
            <xs:element name="MobileCallback" type="xs:boolean" minOccurs="0" />
            <xs:element name="Receptionist" type="xs:boolean" minOccurs="0" />
            <xs:element name="SoftPhone" type="xs:boolean" minOccurs="0" />
            <xs:element name="OneXTelecommuter" type="xs:boolean" minOccurs="0" />
            <xs:element name="AssignedPackage" type="xs:int" minOccurs="0" />
            <xs:element name="AutoRecMode" type="xs:int" minOccurs="0" />
            <xs:element name="CallLogTimeout" type="xs:string" minOccurs="0" />
            <xs:element name="UserCLI" type="xs:string" minOccurs="0" />
        </xs:sequence>
        <xs:attribute name="GUID" type="xs:string" />
    </xs:complexType>

    <xs:complexType name="xmlDSSKeys">
        <xs:sequence>
            <xs:element minOccurs="0" maxOccurs="unbounded" name="DSSKey"
                type="csm:xmlDSSKey"/>

        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlDSSKey">
        <xs:sequence>
            <xs:element name="KeyType" type="xs:int" minOccurs="0"/>
            <xs:element name="Label" type="xs:string" minOccurs="0" />
            <xs:element name="ActionObject" type="xs:string" minOccurs="0" />
            <xs:element name="Data" type="xs:string" minOccurs="0" />
            <xs:element name="RingDelay" type="xs:int" minOccurs="0" />
            <xs:element name="IdlePos" type="xs:string" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="Key" type="xs:int" />
    </xs:complexType>


    <xs:complexType name="xmlShortCodes">
        <xs:sequence>
            <xs:element minOccurs="0" maxOccurs="unbounded" name="ShortCode"
                type="csm:xmlShortCode"  />

        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlShortCode">
        <xs:sequence>
            <xs:element name="Code" type="xs:string" minOccurs="0" />
            <xs:element name="TelephoneNumber" type="xs:string" minOccurs="0" />
            <xs:element name="LineGroupId" type="xs:int" minOccurs="0" />
            <xs:element name="Feature" type="xs:string" minOccurs="0" />
            <xs:element name="Locale" type="xs:string" minOccurs="0" />
            <xs:element name="ForceAccountCode" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForceAuthCode" type="xs:boolean" minOccurs="0" />
        </xs:sequence>
        <xs:attribute name="GUID" type="xs:string" />
    </xs:complexType>

    <xs:complexType name="xmlVoip">
        <xs:sequence>
            <xs:element name="GatekeeperPrimaryIPAddress" type="xs:string"
minOccurs="0" />
```

```
            <xs:element name="GatekeeperSecondaryIPAddress" type="xs:string"
minOccurs="0" />
            <xs:element name="IPAddress" type="xs:string" minOccurs="0" />
            <xs:element name="EnableFaststart" type="xs:boolean" minOccurs="0" />
           <xs:element name="FaxTransportSupport" type="xs:boolean" minOccurs="0" />
            <xs:element name="LocalHoldMusic" type="xs:boolean" minOccurs="0" />
            <xs:element name="LocalTones" type="xs:boolean" minOccurs="0" />
            <xs:element name="RSVPEnabled" type="xs:boolean" minOccurs="0" />
            <xs:element name="OOB_DTMF" type="xs:boolean" minOccurs="0" />
            <xs:element name="AllowDirectMedia" type="xs:boolean" minOccurs="0" />
            <xs:element name="H450Support" type="xs:int" minOccurs="0" />
            <xs:element name="AnnexlSupport" type="xs:boolean" minOccurs="0" />
            <xs:element name="InputGain" type="xs:int" minOccurs="0" />
            <xs:element name="OutputGain" type="xs:int" minOccurs="0" />
            <xs:element name="MediaSecurity" type="xs:int" minOccurs="0" />
           <xs:element name="RTP_Authentication" type="xs:boolean" minOccurs="0" />
            <xs:element name="RTP_Encryption" type="xs:boolean" minOccurs="0" />
           <xs:element name="RTCP_Authentication" type="xs:boolean" minOccurs="0" />
            <xs:element name="RTCP_Encryption" type="xs:boolean" minOccurs="0" />
            <xs:element name="SRTP_Window_Size" type="xs:string" minOccurs="0" />
           <xs:element name="Crypto_Suite_SHA_80" type="xs:boolean" minOccurs="0" />
           <xs:element name="Crypto_Suite_SHA_32" type="xs:boolean" minOccurs="0" />

        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlSipExtn">
        <xs:sequence>
           <xs:element name="ForceAuthentication" type="xs:boolean" minOccurs="0" />
            <xs:element name="Rel100Supported" type="xs:string" minOccurs="0" />

        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlExtnDS">
        <xs:sequence>
           <xs:element name="AdmmUseHandsetConfig" type="xs:boolean" minOccurs="0" /
>
            <xs:element name="AdmmType" type="xs:int" minOccurs="0" />
            <xs:element name="AdmmIpei" type="xs:int" minOccurs="0" />
            <xs:element name="AdmmAnonymous" type="xs:boolean" minOccurs="0" />

        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlT38Fax">
        <xs:sequence>
            <xs:element name="Defaulted" type="xs:string" minOccurs="0" />
            <xs:element name="T38FaxVersion" type="xs:string" minOccurs="0" />
            <xs:element name="RedundancyLowSpeed" type="xs:string" minOccurs="0" />
           <xs:element name="RedundancyHighSpeed" type="xs:string" minOccurs="0" />
            <xs:element name="NSFOveride" type="xs:string" minOccurs="0" />
            <xs:element name="NSFCountryCode" type="xs:string" minOccurs="0" />
            <xs:element name="NSFVendorCode" type="xs:string" minOccurs="0" />
            <xs:element name="TxNetworkTimeout" type="xs:string" minOccurs="0" />
            <xs:element name="ScanLineFixup" type="xs:string" minOccurs="0" />
            <xs:element name="TopEnhancement" type="xs:string" minOccurs="0" />
            <xs:element name="DisableT30ECM" type="xs:string" minOccurs="0" />
            <xs:element name="DisableT30MR" type="xs:string" minOccurs="0" />
            <xs:element name="DisableEFlagsForFirstDis" type="xs:string"
minOccurs="0" />
            <xs:element name="EflagStartTimer" type="xs:string" minOccurs="0" />
            <xs:element name="EflagStopTimer" type="xs:string" minOccurs="0" />
            <xs:element name="FaxTransport" type="xs:string" minOccurs="0" />
            <xs:element name="TCFMethod" type="xs:int" minOccurs="0" />
```

```
            <xs:element name="MaxFaxRate" type="xs:int" minOccurs="0" />

        </xs:sequence>
    </xs:complexType>



</xs:schema>
```

Sample XML for the Avaya Branch Gateway Communication Profiles

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"  xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/
schema/import userimport.xsd" >
 <tns:user>
 <authenticationType>BASIC</authenticationType>
 <givenName>user9000</givenName>
 <loginName>user9000@avaya.com</loginName>
 <middleName>middleName</middleName>
 <surname>surname</surname>
 <userPassword>userPassword</userPassword>
 <commPassword>commPassword</commPassword>
 <commProfileSet>
 <commProfileSetName>commProfileSetName5200</commProfileSetName>
 <isPrimary>true</isPrimary>
 <commProfileList>
 <commProfile xsi:type="csm:xmlB5800UserProfile"  xmlns:csm="http://xml.avaya.com/
schema/import_csm_b5800">
     <commProfileType>B5800 Branch Gateway</commProfileType>
    <csm:deviceName>ABG_178_163</csm:deviceName>
    <csm:userTemplate>userinfo</csm:userTemplate>
    <csm:extension>9000</csm:extension>
    <csm:extensionType>Sip</csm:extensionType>
    <csm:deleteExtOnUserDelete>true</csm:deleteExtOnUserDelete>
</commProfile>
</commProfileList>
 </commProfileSet>
 </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of global setting records

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ext="http://
xml.avaya.com/schema/import" xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://xml.avaya.com/schema/import" version="1.0">
    <xs:annotation>
        <xs:documentation xml:lang="en">
          This Schema defines schema for bulk import and export of System ACL,Public
Contacts and Shared Address.
        </xs:documentation>
    </xs:annotation>
    <xs:element name="presenceSystemDefault" type="tns:xmlPresSystemDefaultType"/>
    <xs:element name="presenceEnforcedUserACL"
type="tns:xmlPresEnforcedUserACLEntryType"/>
    <xs:element name="presenceSystemRule" type="tns:xmlPresSystemRuleType"/>
    <xs:element name="presenceSystemACL" type="tns:xmlPresSystemACLEntryType"/>
    <xs:element name="publicContact" type="tns:xmlPublicContact"/>
    <xs:element name="globalSettings" type="tns:globalSettingsType"/>
    <xs:element name="sharedAddress" type="tns:xmlSharedAddress"/>
    <xs:complexType name="globalSettingsType">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            ---Root Element 'presenceSystemDefault' represent a global default that
```

```
defines access to presence if none of the more specific rules apply. There must be
at least one System Default rule defined.
            ---Root Element 'presenceEnforcedUserACL' represent collection of
Enforced User ACL (containing 1 or more Enforced User ACL).This rule is similar to
a User ACL in the sense that its entries define access between individual
presentities and watchers. However this rule is managed by the administrator as
opposed to presentities themselves. Entries of Enforced User ACL can also be defined
with different priorities. Entries with higher priority will have more weight than
entries with lower priority.
          ---Root Element 'presenceSystemRule' represent collection of System Rules
(containing 1 or more System Rules).Global rules that enforce certain level of
presence access for everyone in the solution. There may be several rules that apply
to all presentities and all watchers. System Rules are used to enforce global
policies. For example, a system rule can declare that telephony presence should be
available to everybody in the company. System Rules can be defined with different
priorities. Rules with higher priority will have more weight than rules with lower
priority
            ---Root Element 'presenceSystemACL' represent collection of System ACL
(containing 1 or more System ACL).System ACL (Access Control List) – are enterprise-
wide rules that can allow a watcher to see presence of all users or deny a watcher
from accessing anyone's presence.  There may be several entries in the list, each
entry corresponding to one watcher. System ACL is normally used to provide critical
system services with a privileged access to presence of all users.
           ---Root Element 'publicContact' represent collection of public contacts
(containing 1 or more public contacts).A personal contact is owned by an individual
user and is not accessible to all users. A public contact can be shared by all users
and is owned by the default system user.
            ---Root Element 'sharedAddress' represent collection of  shared Address
(containing 1 or more shared Addresses).A shared Address can be shared by all users.
        </xs:documentation>
    </xs:annotation>
        <xs:sequence>
            <xs:element name="presenceSystemDefault"
type="tns:xmlPresSystemDefaultType" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceEnforcedUserACL"
type="tns:xmlPresEnforcedUserACLEntryType" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceSystemRule" type="tns:xmlPresSystemRuleType"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceSystemACL"
type="tns:xmlPresSystemACLEntryType" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="sharedAddress" type="tns:xmlSharedAddress"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="publicContact" type="tns:xmlPublicContact"
minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlSharedAddress">
        <xs:sequence>
            <xs:annotation>
                <xs:documentation xml:lang="en">
                  ---addressType:The unique text name of the address type. Possible
values are: Home, business.
                   ---name: The Name property defines the unique label by which the
address is known. Default format for user specific address should include user name
place address type.
                    ---building:The name or other designation of a structure.
                    ---localityName:The name of a locality, such as a city, county
or other geographic region.
                   ---postalCode:A code used by postal services to route mail to a
destination. In the United States this is the zip code.
                    ---room:Name or designation of a room.
                    ---stateOrProvince:The full name of a state or province.
                    ---country:A country.
                   ---street:The physical address of the object such as an address
for package delivery
```

```
                ---postalAddress:A free formed text area for the complete physical
delivery address. It may be used in place of the specific fields in this table.
                ---readOnly:A boolean indicator showing whether or not the address
can be changed from its default value.
              </xs:documentation>
            </xs:annotation>
            <xs:element name="addressType" type="xs:string"/>
            <xs:element name="name" type="xs:string"/>
            <xs:element name="building" type="xs:string" minOccurs="0"/>
            <xs:element name="localityName" type="xs:string" minOccurs="0"/>
            <xs:element name="postalCode" type="xs:string" minOccurs="0"/>
            <xs:element name="room" type="xs:string" minOccurs="0"/>
            <xs:element name="stateOrProvince" type="xs:string" minOccurs="0"/>
            <xs:element name="country" type="xs:string" minOccurs="0"/>
            <xs:element name="street" type="xs:string" minOccurs="0"/>
            <xs:element name="postalAddress" minOccurs="0">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:maxLength value="1024"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="readOnly" type="xs:boolean" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPublicContact">
        <xs:sequence>
            <xs:annotation>
                <xs:documentation xml:lang="en">
                    ---company:The organization that the contact belongs to.
                  ---description: A free text field containing human readable text
providing information on this entry.
                    ---displayName:The localized name of a contact to be used when
displaying. It will typically be the localized full name. This value may be
provisioned from the user’s enterprise directory entry. If it does not exist,
synchronization rules can be used to populate it for other fields e.g. Surname,
GivenName, or LoginName.
                  ---displayNameAscii:The full text name of the contact represented
in ASCII. It is used to support display (e.g. endpoints) that cannot handle
localized text.
                    ---dn:The distinguished name of the user. The DN is a sequence
of relative distinguished names (RDN) connected by commas. An RDN is an attribute
with an associated value in the form of attribute=value, normally expressed in a
UTF-8 string format. The dn can be used to uniquely identify this record. Note the
dn is changeable.
                    ---givenName:The first name of the contact.
                    ---initials:Initials of the contact.
                    ---middleName:The middle name of the contact.
                    ---preferredGivenName:The nick name of the contact.
                  ---preferredLanguage:The individual's preferred written or spoken
language. Values will conform to rfc4646 and the reader should refer to rfc4646 for
syntax.  This format uses the ISO standard Language (ISO-639) and region (ISO-3166)
codes In the absence of a value the client’s locale should be used, if no value is
set, en-US should be defaulted.
                   ---source:Free format text field that identifies the entity that
created this user record.  The format of this field will be either a IP Address/Port
or a name representing an enterprise LDAP or Avaya.
                    ---sourceUserKey:The key of the user from the source system. If
the source is an Enterprise Active Directory server, this value with be the
objectGUID.
                    ---suffix:The text appended to a name e.g. Jr., III.
                    ---surname:The user's last name, also called the family name.
                    ---title:The job function of a person in their organizational
context.Examples: supervisor, manager.
                    ---contactAddresses:A Entity used to store a contact’s address.
```

```
                    ---addresses:A fully qualified URI for interacting with this
contact. Any addresses added to this entity should contain a qualifier e.g. sip,
sips, tel, mailto. The address should be syntactically valid based on the qualifier.
It must be possible to add via the GUI and Interface. The application must do
validation.
                </xs:documentation>
            </xs:annotation>
            <xs:element name="company" type="xs:string" minOccurs="0"/>
            <xs:element name="description" type="xs:string" minOccurs="0"/>
            <xs:element name="displayName" type="xs:string"/>
            <xs:element name="displayNameAscii" type="xs:string"/>
            <xs:element name="dn" type="xs:string" minOccurs="0"/>
            <xs:element name="givenName" type="xs:string"/>
            <xs:element name="initials" type="xs:string" minOccurs="0"/>
            <xs:element name="middleName" type="xs:string" minOccurs="0"/>
            <xs:element name="preferredGivenName" type="xs:string" minOccurs="0"/>
            <xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
            <xs:element name="source" type="xs:string"/>
            <xs:element name="sourceUserKey" type="xs:string"/>
            <xs:element name="suffix" type="xs:string" minOccurs="0"/>
            <xs:element name="surname" type="xs:string"/>
            <xs:element name="title" type="xs:string" minOccurs="0"/>
            <xs:element name="contactAddresses" type="tns:xmlContactAddressList"
minOccurs="0"/>
            <xs:element name="addresses" type="tns:xmlAddressList" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContactAddressList">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                  ContactAddressList: A list containing Contact Addresses
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="contact" type="tns:xmlContactAddress" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContactAddress">
        <xs:sequence>
            <xs:annotation>
                <xs:documentation xml:lang="en">
                   ---type:The value reflecting the type of handle this is. Possible
values are “username”, ”e164”, and “privatesubsystem
                     ---category:The value representing a further qualification to
the contact address. Possible values inlcude Office, Home, Mobile.
                  ---handle:This is the name given to the user to allow communication
to be established with the user. It is an alphanumeric value that must comply with
the userinfo related portion of a URI as described in rfc2396. However, it is
further restricted as ASCII characters with only the “+” prefix to signify this is
an E.164 handle and "_" and "." special characters supported.The handle and type
together are unique within a specific domain. Note, the handle plus domain can be
used to construct a user’s Address of Record.
                     ---label:A free text description for classifying this contact.
                   ---altLabel:A free text description for classifying this contact.
This is similar to ContactLabel, but it is used to store alternate language
representations.
                </xs:documentation>
            </xs:annotation>
            <xs:element name="type" type="xs:string"/>
            <xs:element name="category" type="xs:string" minOccurs="0"/>
            <xs:element name="handle" type="xs:string"/>
            <xs:element name="label" type="xs:string" minOccurs="0"/>
            <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
        </xs:sequence>
```

```
    </xs:complexType>
    <xs:complexType name="xmlAddressList">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                  AddressList: A list containing Addresses
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="address" type="tns:xmlAddress" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlAddress">
        <xs:complexContent>
            <xs:extension base="tns:xmlSharedAddress">
                <xs:sequence>
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                           private:A boolean indicator to specify if this attribute
set could be shared across multiple users. Private attributes sets can only be owned
by a single user. Default=false.
                        </xs:documentation>
                    </xs:annotation>
                    <xs:element name="private" type="xs:boolean"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresInfoTypeAccessType">
        <xs:sequence>
            <xs:annotation>
                <xs:documentation xml:lang="en">
                     ---accessLevel:possible values:IM,Telephony
                  ---action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING,
UNDEFINED
                </xs:documentation>
            </xs:annotation>
            <xs:element name="accessLevel" type="xs:string"/>
            <xs:element name="action" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPresACRuleType">
        <xs:sequence>
            <xs:element name="infoTypeAccess" type="tns:xmlPresInfoTypeAccessType"
minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPresSystemDefaultType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                'presenceSystemDefault' represent a global default that defines
access to presence if none of the more specific rules apply. There must be at least
one System Default rule defined.
            </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType"/>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresSystemRuleType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType">
                <xs:sequence>
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
```

```
                          --- 'presenceSystemRule' represent collection of System
Rules (containing 1 or more System Rules).Global rules that enforce certain level
of presence access for everyone in the solution. There may be several rules that
                           apply to all presentities and all watchers. System Rules
are used to enforce global policies. For example, a system rule can declare that
telephony presence should be available to everybody in the company. System
                         Rules can be defined with different priorities. Rules with
higher priority will have more weight than rules with lower priority apply to all
presentities and all watchers.
                       ---priority:Entries of Enforced User ACL can also be defined
with different priorities. Entries with higher priority will have more weight than
entries with lower priority.
                            </xs:documentation>
                    </xs:annotation>
                    <xs:element name="priority" type="xs:string"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresSystemACLEntryType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType">
                <xs:sequence>
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                          ---'presenceSystemACL' represent collection of System ACL
(containing 1 or more System ACL).System ACL (Access Control List) – are enterprise-
wide rules that can allow a watcher to see presence of all users or deny a watcher
from accessing anyone's presence.  There may be several entries in the list, each
entry corresponding to one watcher. System ACL is normally used to provide critical
system services with a privileged access to presence of all users.
                           ---watcherLoginName:LoginName of the watcher. This value
needs to be specified if watcher is a user.
                            ---watcherDisplayName:DisplayName of the watcher. This
value needs to be specified if watcher is a Contact
                            </xs:documentation>
                    </xs:annotation>
                    <xs:choice>
                        <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
                        <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
                    </xs:choice>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresEnforcedUserACLEntryType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType">
                <xs:sequence>
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                          ---'presenceEnforcedUserACL' represent collection of
Enforced User ACL (containing 1 or more Enforced User ACL).This rule is similar to
a User ACL in the sense that its entries define access between individual
presentities and watchers. However this rule is managed by the administrator as
opposed to presentities themselves. Entries of Enforced User ACL can also be defined
with different priorities. Entries with higher priority will have more weight than
entries with lower priority.
                           ---watcherLoginName:LoginName of the watcher. This value
needs to be specified if watcher is a user.
                            ---watcherDisplayName:DisplayName of the watcher. This
value needs to be specified if watcher is a Contact
                            ---priority:Entries of Enforced User ACL can also be
```

```
defined with different priorities. Entries with higher priority will have more
weight than entries with lower priority.
                           ---userName:LoginName of the presentity.
                         </xs:documentation>
                    </xs:annotation>
                    <xs:element name="userName" type="xs:string"/>
                    <xs:choice>
                        <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
                        <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
                    </xs:choice>
                    <xs:element name="priority" type="xs:string"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
</xs:schema>
```

Sample XML for bulk import of global setting records

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:globalSettings xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/import systemPresence.xsd ">

  <!-- Root Element 'presenceSystemDefault' represent a global default that defines
access to presence if none of the more specific rules apply. There must be at least
one System Default rule defined.
     accessLevel:possible values:ALL,Telephony
     action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
  -->
  <tns:presenceSystemDefault>
      <infoTypeAccess>
        <accessLevel>ALL</accessLevel>
        <action>ALLOW</action>
      </infoTypeAccess>
    </tns:presenceSystemDefault>
   <!--Root Element 'presenceEnforcedUserACL' represent collection of Enforced User
ACL (containing 1 or more Enforced User ACL).This rule is similar to a User ACL in
the sense that its entries define access between individual      presentities
and watchers. However this rule is managed by the administrator as opposed to
presentities themselves. Entries of Enforced User ACL can also be defined with
different priorities. Entries with higher priority will have more weight than
entries with lower priority.
     accessLevel:possible values:ALL,Telephony
     action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
     watcherLoginName:LoginName of the watcher. This value needs to be specified if
watcher is a user.
     watcherDisplayName:DisplayName of the watcher. This value needs to be specified
if watcher is a Contact
     priority:Entries of Enforced User ACL can also be defined with different
priorities. Entries with higher priority will have more weight than entries with
lower priority.
       userName:LoginName of the presentity.
-->
    <tns:presenceEnforcedUserACL>
      <infoTypeAccess>
        <accessLevel>Telephony</accessLevel>
        <action>BLOCK</action>
      </infoTypeAccess>
      <userName>jmiller@avaya.com</userName>
      <watcherLoginName>userlogin2@avaya.com</watcherLoginName>
      <priority>HIGH</priority>
    </tns:presenceEnforcedUserACL>
```

```
    <!--    Root Element 'presenceSystemRule' represent collection of System Rules
(containing 1 or more System Rules).Global rules that enforce certain level of
presence access for everyone in the solution. There may be several rules that apply
to all presentities and all watchers. System Rules are used to enforce global
policies. For example, a system rule can declare that telephony presence should be
available to everybody in the company. System Rules can be defined with different
priorities. Rules with higher priority will have more weight than rules with lower
priority
    accessLevel:possible values:IM,Telephony
     action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
     watcherLoginName:LoginName of the watcher. This value needs to be specified if
watcher is a user.
     watcherDisplayName:DisplayName of the watcher. This value needs to be specified
if watcher is a Contact
     priority:Entries of Enforced User ACL can also be defined with different
priorities. Entries with higher priority will have more weight than entries with
lower priority.
    -->
    <tns:presenceSystemRule>
      <infoTypeAccess>
        <accessLevel>Telephony</accessLevel>
        <action>ALLOW</action>
      </infoTypeAccess>
      <priority>HIGH</priority>
    </tns:presenceSystemRule>
   <!--Root Element 'presenceSystemACL' represent collection of System ACL
(containing 1 or more System ACL).System ACL (Access Control List) – are enterprise-
wide rules that can allow a watcher to see presence of all users or     deny a
watcher from accessing anyone's presence.  There may be several entries in the list,
each entry corresponding to one watcher. System ACL is normally used to provide
critical system services with a privileged access to presence of all users.
     accessLevel:possible values:IM,Telephony
     action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
     watcherLoginName:LoginName of the watcher. This value needs to be specified if
watcher is a user.
  -->
    <tns:presenceSystemACL>
      <infoTypeAccess>
        <accessLevel>Telephony</accessLevel>
        <action>BLOCK</action>
      </infoTypeAccess>
      <watcherLoginName>jmiller@avaya.com</watcherLoginName>
    </tns:presenceSystemACL>
  <!--Root Element 'publicContact' represent collection of public contacts
(containing 1 or more public contacts).A personal contact is owned by an individual
user and is not accessible to all users. A public contact can be shared by all users
and is owned by the default system user.
   company:The organization that the contact belongs to.
    description: A free text field containing human readable text providing
information on this entry.
    displayName:The localized name of a contact to be used when displaying. It will
typically be the localized full name. This value may be provisioned from the user’s
enterprise directory entry. If it does not exist, synchronization rules can be used
to populate it for other fields e.g. Surname, GivenName, or LoginName.
    displayNameAscii:The full text name of the contact represented in ASCII. It is
used to support display (e.g. endpoints) that cannot handle localized text.
    dn:The distinguished name of the user. The DN is a sequence of relative
distinguished names (RDN) connected by commas. An RDN is an attribute with an
associated value in the form of attribute=value, normally expressed in a UTF-8
string format. The dn can be used to uniquely identify this record. Note the dn is
changeable.
    givenName:The first name of the contact.
    initials:Initials of the contact.
    middleName:The middle name of the contact.
    preferredGivenName:The nick name of the contact.
```

```
    preferredLanguage:The individual's preferred written or spoken language. Values
will conform to rfc4646 and the reader should refer to rfc4646 for syntax.  This
format uses the ISO standard Language (ISO-639) and region (ISO-3166) codes In the
absence of a value the client’s locale should be used, if no value is set, en-US
should be defaulted.
    source:Free format text field that identifies the entity that created this user
record.  The format of this field will be either a IP Address/Port or a name
representing an enterprise LDAP or Avaya.
    sourceUserKey:The key of the user from the source system. If the source is an
Enterprise Active Directory server, this value with be the objectGUID.
    suffix:The text appended to a name e.g. Jr., III.
    surname:The user's last name, also called the family name.
    title:The job function of a person in their organizational context.Examples:
supervisor, manager.
    contactAddresses:A table used to store a contact’s address.
    addresses:A fully qualified URI for interacting with this contact. Any addresses
added to this table should contain a qualifier e.g. sip, sips, tel, mailto. The
address should be syntactically valid based on the qualifier. It must be possible
to add via the GUI and Interface. The application must do validation.
    -->
    <tns:publicContact>
      <company>ABC</company>
      <description>Company ABC description</description>
      <displayName>John Miller</displayName>
      <displayNameAscii></displayNameAscii>
      <dn>dc=acme,dc=org</dn>
      <givenName>John</givenName>
      <initials>Mr</initials>
      <middleName>M</middleName>
      <preferredGivenName>John</preferredGivenName>
      <preferredLanguage>English</preferredLanguage>
      <source>ldap</source>
      <sourceUserKey>18966</sourceUserKey>
      <suffix>Jr.</suffix>
      <surname>Miller</surname>
      <title>Manager</title>
      <!--type:The value reflecting the type of handle this is. Possible values are
“username”, ”e164”, and “privatesubsystem
        category:The value representing a further qualification to the contact
address. Possible values inlcude Office, Home, Mobile.
        handle:This is the name given to the user to allow communication to be
established with the user. It is an alphanumeric value that must comply with the
userinfo related portion of a URI as described in rfc2396. However, it is further
restricted as ASCII characters with only the “+” prefix to signify this is an E.164
handle and "_" and "." special characters supported.The handle and type together are
unique within a specific domain. Note, the handle plus domain can be used to
construct a user’s Address of Record.
        label:A free text description for classifying this contact.
        altLabel:A free text description for classifying this contact. This is
similar to ContactLabel, but it is used to store alternate language representations.
    -->
      <contactAddresses>
        <contact>
          <type>sip</type>
          <category>office</category>
          <handle>sip:jmiller@abc.com</handle>
          <label>Miller</label>
          <altLabel>John</altLabel>
        </contact>
      </contactAddresses>
      <addresses>
      <!--    addressType:The unique text name of the address type. Possible values
are:   Home, business.
        name: The Name property defines the unique label by which the address is
known. Default format for user specific address should include user name place
```

```
address type.
        building:The name or other designation of a structure.
        localityName:The name of a locality, such as a city, county or other
geographic region.
        postalCode:A code used by postal services to route mail to a destination.
In the United States this is the zip code.
        room:Name or designation of a room.
        stateOrProvince:The full name of a state or province.
        country:A country.
        street:The physical address of the object such as an address for package
delivery
        postalAddress:A free formed text area for the complete physical delivery
address. It may be used in place of the specific fields in this table.
-->
        <address>
          <addressType>office</addressType>
          <name>John Miller</name>
          <building>building A</building>
          <localityName>Magarpatta</localityName>
          <postalCode>411048</postalCode>
          <room>room 123</room>
          <stateOrProvince>MH</stateOrProvince>
          <country>India</country>
          <street>Hadapsar</street>
          <private>false</private>
        </address>
      </addresses>
    </tns:publicContact>
      <!--addressType:The unique text name of the address type. Possible values
are:   Home, business.
        name: The Name property defines the unique label by which the address is
known. Default format for user specific address should include user name place
address type.
        building:The name or other designation of a structure.
        localityName:The name of a locality, such as a city, county or other
geographic region.
        postalCode:A code used by postal services to route mail to a destination.
In the United States this is the zip code.
        room:Name or designation of a room.
        stateOrProvince:The full name of a state or province.
        country:A country.
        street:The physical address of the object such as an address for package
delivery
        postalAddress:A free formed text area for the complete physical delivery
address. It may be used in place of the specific fields in this table.
        readOnly:A boolean indicator showing whether or not the address can be
changed from its default value.
-->
  <tns:sharedAddress>
      <addressType>office</addressType>
      <name>Avaya Pune</name>
        <building>building A</building>
         <localityName>Magarpatta</localityName>
         <postalCode>411048</postalCode>
        <room>room 123</room>
        <stateOrProvince>MH</stateOrProvince>
         <country>India</country>
         <street>Hadapsar</street>
         <readOnly>true</readOnly>
    </tns:sharedAddress>


</tns:globalSettings>
```

XML Schema Definition for bulk deletion of global setting records

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/bulkdelete"
targetNamespace="http://xml.avaya.com/schema/bulkdelete"
          elementFormDefault="qualified" version="1.0" xmlns:xs="http://www.w3.org/
2001/XMLSchema">


    <xs:element name="sharedAddress" type="tns:xmlDeleteSharedAddress"/>
    <xs:element name="publicContact" type="tns:xmlDeletePublicContact" />
    <xs:element name="presenceEnforcedUserACL"
type="tns:xmlDeletePresEnforcedUserACLEntry"/>
    <xs:element name="presenceSystemRule" type="tns:xmlDeletePresSystemRule"/>
    <xs:element name="presenceSystemACL" type="tns:xmlDeletePresSystemACLEntry"/>


    <xs:element name="deleteGlobalSettings">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="sharedAddress" type="tns:xmlDeleteSharedAddress"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="publicContact" type="tns:xmlDeletePublicContact"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceEnforcedUserACL"
type="tns:xmlDeletePresEnforcedUserACLEntry" minOccurs="0" maxOccurs="unbounded"/>
          <xs:element name="presenceSystemRule" type="tns:xmlDeletePresSystemRule"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceSystemACL"
type="tns:xmlDeletePresSystemACLEntry" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
   </xs:element>

   <xs:complexType name="xmlDeleteSharedAddress">
        <xs:sequence>
            <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlDeletePublicContact">
        <xs:sequence>
            <xs:element name="displayName" type="xs:string" maxOccurs="1"
minOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlDeletePresEnforcedUserACLEntry">
        <xs:sequence>
           <xs:element name="userName" type="xs:string" maxOccurs="1" minOccurs="1"/
>
            <xs:choice>
               <xs:element name="watcherLoginName" type="xs:string" minOccurs="0"/>
              <xs:element name="watcherDisplayName" type="xs:string" minOccurs="0"/>
            </xs:choice>
           <xs:element name="priority" type="xs:string" maxOccurs="1" minOccurs="1"/
>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlDeletePresSystemRule">
        <xs:sequence>
                    <xs:element name="priority" type="xs:string" maxOccurs="1"
minOccurs="1"/>
        </xs:sequence>
```

```
    </xs:complexType>

    <xs:complexType name="xmlDeletePresSystemACLEntry">
        <xs:sequence>
            <xs:choice>
                <xs:element name="watcherLoginName" type="xs:string" minOccurs="0"/>
              <xs:element name="watcherDisplayName" type="xs:string" minOccurs="0"/>
            </xs:choice>
        </xs:sequence>
    </xs:complexType>

</xs:schema>
```

Sample XML for bulk deletion of global setting records

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:deleteGlobalSettings xmlns:tns="http://xml.avaya.com/schema/bulkdelete"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/bulkdelete systemPresence_delete.xsd ">

     <tns:presenceSystemRule>
        <tns:priority>LOW</tns:priority>
    </tns:presenceSystemRule>

      <tns:sharedAddress>
        <tns:name>Avaya Pune</tns:name>
      </tns:sharedAddress>

      <tns:publicContact>
        <tns:displayName>John Miller</tns:displayName>
      </tns:publicContact>

      <tns:presenceEnforcedUserACL>
        <tns:userName>jmiller@avaya.com</tns:userName>
        <tns:watcherDisplayName>John Miller</tns:watcherDisplayName>
        <tns:priority>HIGH</tns:priority>
      </tns:presenceEnforcedUserACL>

      <tns:presenceSystemACL>
           <tns:watcherDisplayName>John Miller</tns:watcherDisplayName>
      </tns:presenceSystemACL>

</tns:deleteGlobalSettings>
```

XML Schema Definition for bulk import of roles

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns="http://xml.avaya.com/bulkimport" xmlns:xs="http://www.w3.org/
2001/XMLSchema" targetNamespace="http://xml.avaya.com/bulkimport"
elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            This Schema defines schema for bulk import and export of roles.
            Root Element 'Roles' represent collection of role (containing 1 or more
roles)
        </xs:documentation>
    </xs:annotation>
    <xs:element name="Roles">
        <xs:complexType>
            <xs:sequence>
                <xs:annotation>
                    <xs:documentation xml:lang="en">
                        A role is a collection of access permissions on a resource.
A user's role will determine the permissions that the user receives to access
resources. Examples of Roles:  Contact Center Manager, Agent, Administrator.
```

```
                        New Roles can be added to the data model using an XML file
conforming to this XSD.Existing Roles too can be updated.
                    </xs:documentation>
                </xs:annotation>
                <xs:element name="Role" maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:annotation>
                                <xs:documentation xml:lang="en">
                                   Operation - Element Containing information about
the Operation.The Operation requires to preexist in SMGR database.Examples of
Operation:  'UserManagement/GlobalUserSettings/ACL' ; 'Settings/Plugin Framework' ;
                                    Resource - Element Containing information about
the Resource. A Resource can be a User, Role, Operation, Group,Element.The Resource
requires to preexist in SMGR database.Examples of Resource:  'Auditor' ;
                                </xs:documentation>
                            </xs:annotation>
                            <xs:element name="Operation" minOccurs="0"
maxOccurs="unbounded">
                                <xs:complexType>
                                    <xs:attribute name="ID" type="xs:string"
use="required">
                                        <xs:annotation>
                                            <xs:documentation xml:lang="en">
                                              ID: The ID of the operation.The value
of this tag corresponds to the OperationID. Note that it is very important that this
value is unique across the system
                                            </xs:documentation>
                                        </xs:annotation>
                                    </xs:attribute>
                                </xs:complexType>
                            </xs:element>
                            <xs:element name="Resource" minOccurs="0"
maxOccurs="unbounded">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element name="ResourceAttributes"
minOccurs="0" maxOccurs="unbounded">
                                            <xs:complexType>
                                               <xs:attribute name="ID" type="xs:string"
use="required">
                                                    <xs:annotation>
                                                    <xs:documentation xml:lang="en">
                                                            ResourceAttributesID:
The ID of the ResourceAttributes.This specifies the attributes of a
resource.Examples of ResourceAttributesID:  'ALL' ; 'LoginName' ;'First Name' for
Resource Type 'user'
                                                        </xs:documentation>
                                                    </xs:annotation>
                                                </xs:attribute>
                                            </xs:complexType>
                                        </xs:element>
                                        <xs:element name="Permissions">
                                            <xs:complexType>
                                                <xs:sequence>
                                                    <xs:annotation>
                                                    <xs:documentation xml:lang="en">
                                                            Permission: String value
specifying Permissions that can be assigned to the Resource Type.Examples of
Permission:view,delete
                                                        </xs:documentation>
                                                    </xs:annotation>
                                                    <xs:element name="Permission"
type="xs:string" maxOccurs="unbounded"/>
                                                </xs:sequence>
```

```
                                        </xs:complexType>
                                    </xs:element>
                                </xs:sequence>
                               <xs:attribute name="ResourceType" type="xs:string"
use="required">
                                    <xs:annotation>
                                        <xs:documentation xml:lang="en">
                                            ResourceType: String Value for
specifying Type of the Resource that needs to be imported.
                                        </xs:documentation>
                                    </xs:annotation>
                                </xs:attribute>
                                <xs:attribute name="NativeResourceID"
type="xs:string" use="required">
                                    <xs:annotation>
                                        <xs:documentation xml:lang="en">
                                        NativeResourceID: Native ID of the Resource.
                                        </xs:documentation>
                                    </xs:annotation>
                                </xs:attribute>
                            </xs:complexType>
                        </xs:element>
                    </xs:sequence>
                  <xs:attribute name="CanAccessAllOperations" type="xs:boolean"
use="required">
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                             CanAccessAllOperations - Boolean value specifying
whether this role can access all operations.
                        </xs:documentation>
                    </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="IsServices" type="xs:boolean" use=
"required" >
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                             IsServices - Boolean value specifying whether this
Role is a  Services Role.
                        </xs:documentation>
                    </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="isDefault" type="xs:boolean"
use="required">
                        <xs:annotation>
                             <xs:documentation xml:lang="en">
                                  isDefault - Boolean value specifying whether
this Role is a  System Role.These Roles can not be deleted.
                            </xs:documentation>
                        </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="Name" type="xs:string" use="required">
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                                  Name - String value specifying Role name.
                        </xs:documentation>
                    </xs:annotation>
                    </xs:attribute>
                   <xs:attribute name="AllResourcesPermission" type="xs:string"
use="optional">
                        <xs:annotation>
                            <xs:documentation xml:lang="en">
                             AllResourcesPermission - String value representing
the comma separated permission strings. These permissions will be applied to all
Resources in the system. The users assigned to this role will get the specified
permissions for all resources. Examples of Resource:'view,delete'
```

```
                                </xs:documentation>
                            </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="Description" type="xs:string"
use="optional">
                        <xs:annotation>
                            <xs:documentation xml:lang="en">
                                      Description - String value specifying Role
description.
                            </xs:documentation>
                        </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="isNHIRole" type="xs:boolean"
use="required">
                            <xs:annotation>
                                <xs:documentation xml:lang="en">
                                      isNHIRole - Boolean value specifying whether
this Role is a  non human interface (nhi) role.
                                </xs:documentation>
                            </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="shareRoles" type="xs:boolean"
use="optional">
                            <xs:annotation>
                                <xs:documentation xml:lang="en">
                                      shareRoles - Boolean value specifying whether
this Role is a  shared role across applications.
                                </xs:documentation>
                            </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="hasFullAccess" type="xs:boolean"
use="optional">
                            <xs:annotation>
                                <xs:documentation xml:lang="en">
                                      hasFullAccess - Boolean value specifying full
access over all resources.Examples of Role with full access : 'System
Administrator' ;
                                </xs:documentation>
                            </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="ApplicationId" type="xs:string"
use="required">
                             <xs:annotation>
                                <xs:documentation xml:lang="en">
                                  ApplicationId - The value of this tag corresponds
to the ApplicationID.Examples of ApplicationId: 'SMGR' ;
                                </xs:documentation>
                            </xs:annotation>
                        </xs:attribute>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

Sample XML for bulk import of roles

```
<?xml version="1.0" encoding="UTF-8"?>
<!--  Root Element 'Roles' represent collection of role (containing 1 or more
roles)-->
<Roles xsi:schemaLocation="http://xml.avaya.com/bulkimport BulkImport.xsd"
xmlns="http://xml.avaya.com/bulkimport" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
    <!--   A role is a collection of access permissions on a resource. A user's role
```

```
will determine the permissions that the user receives to access resources.
    CanAccessAllOperations: Boolean value specifying whether this role can access
all operations.
    IsServices: Boolean value specifying whether this Role is a  Services Role.
    isDefault: Boolean value specifying whether this Role is a  System Role.These
Roles can not be deleted.
    Name: String value specifying Role name.
   AllResourcesPermission:String value representing the comma separated permission
strings. These permissions will be applied to all Resources in the system. The users
assigned to this role will get the specified permissions for all resources.
    Description:String value specifying Role description.
    isNHIRole:Boolean value specifying whether this Role is a  non human interface
(nhi) role.
    shareRoles: Boolean value specifying whether this Role is a  shared role across
applications.
    hasFullAccess:Boolean value specifying full access over all resources.
    ApplicationId:The value of this tag corresponds to the ApplicationID.Examples
of ApplicationId: 'SMGR'
    -->
    <Role CanAccessAllOperations="true" IsServices="true" isDefault="false"
Name="test-role" AllResourcesPermission="view,delete" Description="System
Administrator Role" isNHIRole="false" shareRoles="true"
hasFullAccess="false"            ApplicationId="SMGR" >
    <!--Element Containing information about the Operation.The Operation requires
to preexist in SMGR database.
   ID: The ID of the operation.The value of this tag corresponds to the OperationID.
Note that it is very important that this value is unique across the system    -->
         <Operation ID="GroupsAndRoles/RBAC/ViewRole"/>
             <!--Resource : Element Containing information about the Resource. A
Resource can be a User, Role, Operation, Group,Element.The Resource requires to
preexist in SMGR database.
                 ResourceType: String Value for specifying Type of the Resource that
needs to be imported.
                  NativeResourceID: Native ID of the Resource. -->
            <Resource ResourceType="alarmoperation"
NativeResourceID="ChangeStatusAll">
            <!-- ResourceAttributesID: The ID of the ResourceAttributes.This
specifies the attributes of a resource -->
        <ResourceAttributes ID="ALL" />
           <!--Permission: String value specifying Permissions that can be assigned
to the Resource Type.-->
            <Permissions>
            <Permission>view</Permission>
        </Permissions>
        </Resource>
    </Role>
</Roles>
```

Attribute details defined in Import user XSD

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
authenticationType	This defines the type of authentication the user undergoes at runtime to gain access to the system.	Mandatory	Possible values: • BASIC • ENTERPRISE

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
description	This is a text description of the user; a human readable description of this user instance.	Optional	
displayName	This is the localized name of the user to be used when displaying. Typically, the value is the localized full name. This value might be provisioned from the enterprise directory entry of the user. If the value does not exist, you can use synchronization rules to populate the value for other fields. For example: Surname, GivenName, or LoginName.	Optional	
displayNameAscii	This corresponds to the console attribute Endpoint Display Name. This is the full text name of the user represented in ASCII. It is used to support display (e.g. endpoints) that cannot handle localized text.	Optional	
dn	This is the distinguished name (DN) of the user. DN is a sequence of relative distinguished names (RDN) connected by commas. RDN is an attribute with an associated value in the form of attribute=value, typically expressed in a UTF-8 string format. DN can be used to identify the user and can be used for authentication subject mapping. Note that DN is changeable.	Optional	
isDuplicatedLoginAllowed	This is a boolean indicator showing whether this user is allowed a duplicate	Optional	Default value is true.

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
	concurrent logins. A true stipulates that the user is allow to have duplicate logins.		
isEnabled	This is a boolean indicator showing whether or not the user is active. Users with AuthenticationType=Basic fails if the value is false. This attribute can be used to disable access between login attempts. You cannot revoke login for a running session. Alternatively, the administrator can always modify the password to disable the user from logging in. A true stipulates this is an active user, a false used for a disabled user.	Optional	Default value is false.
isVirtualUser	A boolean indicator showing whether or not the record is being used for a non-human entity such as an application, service, software agent, etc. You use this attribute where the entity behaves as a user and needs to have subset of the user profile populated. If the entity does not behave as a user and has a different trust relationship, for example, a trust certificate must not be treated as a virtual user. A virtual user can represent an Avaya or an external non-human entity. This attribute is provided as a convenience to track such accounts. A true stipulates this is a virtual users, a false is used for human users.	Optional	Default value is false.

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
givenName	This is the first name of the user.	Mandatory	
honorific	This is the personal title used to address a user. This is typically a social title and not the work title which is contained in the title attribute. This attribute can map to "PersonalTitle".	Optional	
loginName	This is the unique system login name given to the user. It can take the form of username@domain or just username. This might vary across customers. It can be used to help provision default user handles in the CSHandle table. The username is an alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc2396. However, it is further restricted as ASCII characters with only the "_" and "." special characters supported. This is the rfc2798 "uid" attribute.	Mandatory	
middleName	This is the middle name of the user.	Optional	
managerName	This is the text name of the user's manager. This is a free formed field and does not require the user's manager to also be a user of the solution. This attribute was requested to support reporting needs.	Optional	
preferredGivenName	This is the preferred first name of the user.	Optional	
preferredLanguage	This is the individual's preferred written or spoken language. Values	Optional	Possible values:

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
	conforms to rfc4646. Refer to rfc4646 for syntax. This format uses the ISO standard Language (ISO-639) and region (ISO-3166) codes In the absence of a value the locale of the client must be used, if no value is set, en_US must be used as default.		• English (United States) - en_US • Chinese (Simplified) - zh_CN • Japanese (Japan) - ja_JP • Korean (Korea) - ko_KR • French (France) - fr_FR • German (Germany) - de_DE • Italian (Italy) - it_IT • Russian (Russia) - ru_RU • English (United Kingdom) - en_GB • Spanish (Mexico) - es_MX • Portugese (Brazil) - pt_BR • French (Canada) - fr_CA • English (Canada) - en_CA
source	Free format text field that identifies the entity that created this user record. The format of this field must be a IP Address/Port or a name representing an enterprise LDAP or Avaya.	Optional	User Management populates the source field with the name of the file.
sourceUserKey	This is the key of the user from the source system. If the source is an Enterprise Active Directory server,	Optional	By default, the value is none.

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
	this value with be the objectGUID.		
status	This information is to help manage provisioning activities such as correcting or completing the provisioning of a user instance. It can also signify that approval is needed (PENDINGAUTHZ) before a user account is sufficiently configured to be a valid user (PROVISIONED).	Optional	Possible values: AUTHPENDING; PENDINGAUTHZ; PROVISIONED
suffix	This is the text appended to a name e.g. Jr., III.	Optional	
surname	This is the user's last name, also called the family name.	Mandatory	
timeZone	This is the preferred time zone of the user. For example: America/ New_York, Europe/Dublin. The application consuming this information must know how to translate e.g. in Java it is TimeZone.getTimeZone(" Europe/Moscow"); In the absence of a value, the system uses the local services timezone. **Note:** You must consider daylight saving time (DST) and summer time adjustments while using the suggested values for **timeZone**. Typically, you add 1 hour to the offset.	Optional	(-12:0)International Date Line West (-11:0)Midway Island, Samoa (-10:0)Hawaii (-9:0)Alaska (-8:0)Pacific Time (US & Canada); Tijuana (-7:0)Mountain Time (US & Canada); Chihuahua, La Paz (-7:0)Arizona (-6:0)Central Time (US & Canada); Guadalajara, Mexico City (-6:0)Central America; Saskatchewan (-5:0)Indiana (East); Bogota, Lima, Quito (-5:0)Eastern Time (US & Canada) (-4:0)Caracas, La Paz

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
	Note: You cannot use the following characters as is in the xml. Make the following modifications while using them in the import xml files: • less-than character (<) as < < • ampersand character (&) as & • greater-than character (>) as > • double-quote character (") as " • apostrophe or single-quote character (') as '		(-4:0)Atlantic Time (Canada); Santiago, Manaus (-3:30)Newfoundland (-3:0)Georgetown (-3:0)Brasilia, Greenland, Buenos Aires, Montevideo (-2:0)Mid-Atlantic (-1:0)Azores (-1:0)Cape Verde Is. (0:0)Monrovia, Reykjavik (0:0)GMT : Dublin, Edinburgh, Lisbon, London, Casablanca (+1:0)West Central Africa (+1:0)Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels, Sarajevo (+2:0)Harare, Pretoria (+2:0)Amman, Athens, Minsk, Beirut, Cairo, Jerusalem, Helsinki, Windhoek (+3:0)Baghdad, Kuwait, Riyadh, Nairobi, Tbilisi (+3:0)Moscow, St. Petersburg, Volgograd (+3:30)Tehran (+4:0)Abu Dhabi, Muscat, Caucasus Standard Time (+4:0)Baku, Tbilisi, Yerevan (+4:30)Kabul (+5:0)Islamabad, Karachi, Tashkent, Ekaterinburg

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
			(+5:30)Chennai, Kolkata, Mumbai, New Delhi, Sri Jayawardenepura (+5:45)Kathmandu (+6:0)Astana, Dhaka, Almaty, Novosibirsk (+6:30)Rangoon (+7:0)Bangkok, Hanoi, Jakarta, Krasnoyarsk (+8:0)Beijing, Hong Kong, Singapore; Taipei (+8:0)Perth; Irkutsk, Ulaan Bataar (+9:0)Seoul, Osaka, Sapporo, Tokyo (+9:0)Yakutsk (+9:30)Darwin, Adelaide (+10:0)Brisbane, Guam, Port Moresby (+10:0)Canberra, Melbourne, Sydney, Hobart, Vladivostok (+11:0)Magadan, Solomon Is., New Caledonia (+12:0)Auckland, Wellington (+12:0)Fiji, Kamchatka, Marshall Is. (+13:0)Nuku'alofa
title	This is the job function of a person in their organizational context.	Optional	
userName	This is the username portion of the loginName field. It is an alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc2396.	Mandatory	

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
	However, it is further restricted as ASCII characters with only the "_" and "." special characters supported. This is the rfc2798 "uid" attribute.		
userPassword	This is the encrypted password for this user account. A null password is used when the user is authenticated by the enterprise such as with a separate source such as the enterprise LDAP.	Optional	Need not specified value for Enterprise User. If the value is not specified for the Basic user, the user will be disabled.
commPassword	This is the encrypted “subscriber” or communication password with which the user logs can use to authentication with on to any CommProfile SIP and non SIP. This attribute is shared across different communication profiles and thus different communication services.	Optional	
userType	This enumerates the possible primary user application types. A User can be associated with multiple user types.	Optional	Possible values are administrator, communication_user, agent, supervisor, resident_expert, service_technician, lobby_phone
roles	This is the text name of a role. This value must pre-exist in SMGR DB.	Optional	
address	This is the address of the user.	Optional	
securityIdentity	This is the SecurityIdentity is used to hold any additional identities for a user that can be used for authentication such as loginName, Kerberos	Optional	

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
	account name, or X509 certificate name.		
ownedContactLists	It is a collection of internal or external contacts. ContactList is owned by a specific user and has a name that a unique name within the context of its owner.	Optional	The system creates a default contactlist per user.
ownedContacts	It represents a non Avaya application user (external) contact. Contacts can be collected together along with User entities into a contact list. Contacts can be created by an administrator or an end user.	Optional	
presenceUserDefault	These are personal rules that are set by presentities to define how much presence information can be shown to watchers that are not explicitly mentioned in an ACL. There can be one User Default rule per presentity (User), or none.	Optional	
presenceUserACL	These are personal rules defined by presentities themselves on who can monitor their presence information. There might be several entries in the list for a given presentity, each entry corresponding to one watcher.	Optional	
presenceUserCLDefault	This is a personal rule that is set by presentities to define how much presence information can be shown to watchers that belong to the contact list of the user. There can be one User Contact List Default rule	Optional	

Attribute	Attribute Description	Mandatory/ Optional	Validation Constraints
	per presentity (Person) or none.		
commProfileSet	A user has a default Commprofile set. A commprofile set can exist without any handles or commprofiles referencing it. That is, you can create a commprofile set without creating a handle or a commprofile. A commprofile set can contain multiple commprofiles, but only one of each specific type. This is enforced by having the CommProfile uniqueness constraint include type, commprofile_set_id.	Optional	A user has a default commprofile set.
employeeNo	Employee number of the user.	Optional	
department	Department which the employee belongs to.	Optional	
organization	Organization which the employee belongs to.	Optional	
localizedNames	Localized name of the user.	Optional	

Attribute details defined in Delete User XSD

Attribute	Attribute description	Mandatory/Optional	Validation constraints
deleteType	Defines the delete type of the user. If the user selects “soft”, the system does not delete the user record permanently. You can recover the user record. If the user selects “delete”,	Mandatory	Possible values: • soft • delete

Attribute	Attribute description	Mandatory/Optional	Validation constraints
	the system permanently deletes all attributes associated with the user and the links to public contacts and shared addresses.		
loginName	A unique system login name assigned to the user in the format of username@domain or username.	Mandatory	
id	A unique identifier for a user record. The id attribute is included in the XSD for future enhancement. This is not used in System Manager 6.0 release.	Optional	

Attribute details defined in the CM Endpoint profile XSD

Attribute details defined in the CM Endpoint profile XSD

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
CM Name cmName	Name of the Communication Manager system as it appears in 'Applications/ Application Management/ Entities	Mandatory	
Use Existing Extension useExistingExtension	'true' if already created extension is to be used. 'false' if available extension is to be used.	Optional	
Template Name template	Template name to be used to create	Optional	

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	endpoint. Values defined in Template will be used if not provided.		
Set Type setType	Specifies the set type of the endpoint.	Optional	
Port port	Valid values for port.	Optional	01 to 64 First and second numbers are the cabinet number A to E Third character is the carrier 01 to 20 Fourth and fifth characters are the slot number 01 to 32 Sixth and seventh characters are the circuit number x or X Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension has a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) endpoints, as well as for SBS Extensions. IP Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension has an IP set. This is

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			automatically entered for certain IP endpoint set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.
Delete endpoint is unassigned deleteOnUnassign	Whether the endpoint must be deleted if it unassigned from the user.	Optional	
Lock messages feature. lockMessages	Enable/ Disable lock messages feature.	Optional	true/false to enable/ disable lock messages feature.
Coverage Path 1 coveragePath1	A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call.	Optional	Valid values: Path Number between 1-9999, time of day table, t1-t999, or blank.
Coverage Path 2	A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call.	Optional	Valid values: Path Number between 1-9999, time of day table, t1-t999, or blank.
Hunt To Station huntToStation	The extension the system must hunt to for this telephone when the telephone is busy. A endpoint hunting chain can be created by assigning a hunt-to endpoint to a series of telephones.	Optional	
Tenant Number tn	Provides for partitioning of attendant groups and/or endpoints and trunk groups.	Mandatory	Valid values: 1 to 100

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	Typically this is used for multiple tenants in a building or multiple departments within a company or organization.		
Class of Restriction cor	This is used for multiple tenants in a building or multiple departments within a company or organization. This is used for multiple tenants in a building or multiple departments within a company or organization.	Mandatory	Valid values: 0 to 995
Class of Service cos	Class of Service lets you define groups of users and control those groups' access to features.	Mandatory	Valid values: 0 to 15
speakerphone	Controls the behavior of speakerphones.	Optional	Valid values : none, 1-way, 2-way
Display Language displayLanguage	The language that displays on endpoints.	Optional	Time of day is displayed in 24- hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.). unicode: Displays English messages in a 24-hour format . If no Unicode file is installed, displays messages in English by default.
Personalized Ringing Pattern personalizedRinging Pattern	Defines the personalized ringing pattern for the endpoint.		L = 530 Hz, M = 750 Hz, and H = 1060 Hz Valid Entries Usage:

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	Personalized Ringing allows users of some telephones to have one of 8 ringing patterns for incoming calls. For virtual endpoints, this field dictates the ringing pattern on its mapped to physical telephone.		1. MMM (standard ringing) 2. HHH 3. LLL 4. LHH 5. HHL 6. HLL 7. HLH 8. LHL
Message Lamp Extension messageLampExt	The Message Lamp Extension associated with the current extension.	Mandatory	
muteButtonEnabled	Enables or disables the mute button on the endpoint.		
Media Complex Extension mediaComplexExt	When used with Multi-media Call Handling, indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to place either a voice or a data call, and voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.	Optional	Valid Entry Usage A valid BRI data extension For MMCH, enter the extension of the data module that is part of this multimedia complex. H.323 endpoint extension For 4600 series IP Telephones, enter the corresponding H.323 endpoint. For IP Softphone, enter the corresponding H.323 endpoint. If you enter a value in this field, you can register this endpoint for either a road-warrior or elecommuter/Avaya IP Agent application. blank Leave this field blank for single-

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			connect IP applications.
IP Softphone ipSoftphone	Whether this is IP soft phone.	Optional	
Servivable GK Node Name survivableGkNodeName	Survivable GK Node Name identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the H.248 gateways. When you enter a valid IP node name in this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP endpoints register with Communication Manager, this list is sent down in the registration confirm message. The IP endpoint can use the IP address of this Survivable Gatekeeper as the call controller of last resort to register with. Available only if the endpoint type is an H.323 endpoint (46xxor 96xx models).	Optional	Valid Entry Usage Valid IP node name Any valid previously-administered IP node name.

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Survivable class of restriction survivableCOR	Sets a level of restriction for endpoints to be used with the survivable dial plan to limit certain users to only to certain types of calls. You can list the restriction levels in order from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by PIM module of the Integrated Management to communicate with the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for Standard Local Survivability (SLS) on the H.248 gateways. Available for all analog and IP endpoint types.	Optional	Valid Entries Usage emergency - This endpoint can only be used to place emergency calls. Internal - This endpoint can only make intra-switch calls. This is the default. local - This endpoint can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables. toll - This endpoint can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables. unrestricted - This endpoint can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users.
Survivable Trunk Destination survivableTrunkDest	Designates certain telephones as not being allowed to receive incoming trunk calls when the Media Gateway is in survivable mode. This field is used by the PIM module of the Integrated Management to	Optional	Valid Entry Usage: true - Allows this endpoint to be an incoming trunk destination while the Media Gateway is running in survivability mode. This is the default. false - Prevents this endpoint from

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	successfully interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the H.248 gateways. Available for all analog and IP endpoint types.		receiving incoming trunk calls when in survivable mode.
Voice Mail Number voiceMailNumber	Enter the complete Voice Mail Dial Up number.	Optional	String
offPremisesStation	Analog telephones only.	Optional	Valid entries Usage: • true - Enter true if this telephone is not located in the same building with the system. If you enter true, you must complete R Balance Network. • false - Enter false if the telephone is located in the same building with the system. •
dataOption	If a second line on the telephone is administered on the I-2 channel, enter analog. Otherwise, enter data module if applicable or none.	Optional	Valid entries analog, none.
Message Waiting Indicator messageWaitingIndicator	If led or neon, then messageLampExt must be enable otherwise its blank.	Optional	Valid entries: led, neon, none.

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
remoteOfficePhone	Enter true to use this endpoint as an endpoint in a remote office configuration.	Optional	Valid entries: • audix - If LWC is attempted, the messages are stored in AUDIX. • spe - If LWC is attempted, the messages are stored in the system processing element (spe). • none - If LWC is attempted, the messages are not stored.
lwcActivation	Enter true to allow internal telephone users to leave short LWC messages for this extension. If the system has hospitality, enter true for guest-room telephones if the extension designated to receive failed wakeup messages must receive LWC messages that indicate the wakeup calls failed. Enter true if LWC Reception is audix.	Optional	Boolean
activeStationRinging	Active endpoint Ringing	Optional	Valid entries: • single • continuous • if-busy-single • silent
idleActiveRinging	Defines how call rings to the	Optional	Valid entries • continuous - Enter continuous to

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	telephone when it is on-hook.		cause all calls to this telephone to ring continuously. • if-busy-single - Enter if-busysingle to cause calls to this telephone to ring continuously when the telephone is off-hook and idle and calls to this telephone to receive one ring cycle and then ring silently when the telephone is off-hook and active. • silent-if-busy - Enter silent-if-busy to cause calls to ring silently when this endpoint is busy. • single - Enter single to cause calls to this telephone to receive one ring cycle and then ring silently.
switchhookFlash	Must be set to true when the Type field is set to H.323	Optional	Boolean
ignoreRotaryDigits	If this field is true, the short switch-hook flash (50 to 150) from a 2500-type set is ignored.	Optional	Boolean
h320Conversion	H.320 Conversion — Valid entries are true and false (default). This field is optional for non-multimedia	Optional	Boolean

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	complex voice endpoints and for Basic multimedia complex voice endpoints. It is mandatory for Enhanced multimedia complex voice endpoints. Because the system can only handle a limited number of conversion calls, you might need to limit the number of telephones with H.320 conversion. Enhanced multimedia complexes must have this flag set to true.		
serviceLinkMode	The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and the Avaya DEFINITY Server which ends the H.320 protocol. A service link is never used by a Basic mode complex H.320 DVC system. Connecting a service link will take several seconds. When the service link is connected, it uses MMI, VC and system timeslot resources. When the service link is disconnected it does not tie up any	Optional	Valid entries as-needed permenant

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	resources. The Service Link Mode can be administered as either ‘as-needed’ or ‘permanent’ as described below: - As- Needed - Most non-call center multimedia users will be administered with this service link mode. The as-needed mode provides the Enhanced multimedia complex with a connected service link whenever a multimedia call is answered by the endpoint and for a period of 10 seconds after the last multimedia call on the endpoint has been disconnected. Having the service link stay connected for 10 seconds allows a user to disconnect a multimedia call and then make another multimedia call without having to wait for the service link to disconnect and re-establish. - Permanent – Multimedia call center agents and other users who are constantly making or receiving multimedia calls might want to be administered with		

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	this service link mode. The permanent mode service link will be connected during the endpoint's first multimedia call and will remain in a connected state until the user disconnects from their PC's multimedia application or the Avaya DEFINITY Server restarts. This provides a multimedia user with a much quicker video cut-through when answering a multimedia call from another permanent mode endpoint or a multimedia call that has been early answered.		
multimediaMode	There are two multimedia modes, Basic and Enhanced,	Optional	Basic - A Basic multimedia complex consists of a BRIconnected multimedia-equipped PC and a non-BRI-connected multifunction telephone set. Enhanced - An Enhanced multimedia complex consists of a BRI-connected multimediaequipped PC and a non-BRIconnected multifunction telephone.
mwiServedUserType	Controls the auditing or interrogation of a	Optional	Valid entries:

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	served user's message waiting indicator (MWI).		1. fp-mwi - Use if the endpoint is a served user of an fp-mwi message center. 2. qsig-mwi - Use if the endpoint is a served user of a qsig-mwi message center. 3. sip adjuncts - Use if the endpoint is a served user of a sip adjuncts message center. 4. blank - Leave blank if you do not want to audit the served user's MWI or if the user is not a served user of either an fp-mwi or qsigmwi message center.
audixName	The AUDIX associated with the endpoint. Must contain a user-defined adjunct name that was previously administered.	Optional	String
automaticMoves	Automatic Moves allows a DCP telephone to be unplugged from one location and moved to a new location without additional	Optional	Valid entries: 1. always - Enter always and the DCP telephone can be moved anytime without

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	Communication Manager administration. Communication Manager automatically associates the extension to the new port.		additional administration by unplugging from one location and plugging into a new location. 2. once - Enter once and the DCP telephone can be unplugged and plugged into a new location once. After a move, the field is set to done the next time that routine maintenance runs on the DCP telephone. Use once when moving a large number of DCP telephones so each extension is removed from the move list. Use once to prevent automatic maintenance replacement. 3. no - Enter no to require administration in order to move the DCP telephone. 4. done - Done is a display-only value. Communication Manager sets the field to done

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			after the telephone is moved and routine maintenance runs on the DCP telephone. 5. Error - Error is a display-only value. Communication Manager sets the field to error, after routine maintenance runs on the DCP telephone, when a non-serialized telephone is set as a movable telephone.
remoteSoftphoneEmergencyCalls	An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks.	Optional	Valid entries: 1. As-on-local - as-on-local sends the extension entered in the Emergency Location Extension field on the Endpoint screen to the Public Safety Answering Point (PSAP) 2. Block - Enter block to prevent the completion of emergency calls. 3. Cesid - Enter cesid to allow Communication Manager to send the CESID information

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			supplied by the IP Softphone to the PSAP. 4. Option - Enter option to allow the user to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported.
emergencyLocation Ext	This field allows the system to properly identify the location of a caller who dials a 911 emergency call from this endpoint. An entry in this field must be of an extension type included in the dial plan, but does not have to be an extension on the local system. It can be a UDP extension. The entry defaults to blank. A blank entry typically is used for an IP softphone dialing in through PPP from somewhere outside your network. If you populate the IP Address Mapping screen with emergency numbers, the feature functions as follows: If the Emergency Location Extension field in the Endpoint screen is the same as the	Optional	

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	Emergency Location Extension field in the IP Address Mapping screen, the feature sends the extension to the Public Safety Answering Point (PSAP). If the Emergency Location Extension field in the Endpoint screen is different from the Emergency Location Extension field in the IP Address Mapping screen, the feature sends the extension in the IP Address Mapping screen to the Public Safety Answering Point (PSAP).		
alwaysUse	A softphone can register no matter what emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the administered Emergency Location Extension is used. The softphone's user-entered settings are ignored. If an IP telephone dials 911, the administered Emergency Location Extension is used. If a call center agent dials 911, the physical endpoint extension is displayed, overriding the administered LoginID for ISDN Display . Does not	Optional	Boolean

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	apply to SCCAN wireless telephones, or to extensions administered as type h.323.		
precedenceCallWaiting	Activates or deactivates Precedence Call Waiting for this endpoint.	Optional	
autoSelectAnyIdleAppearance	Enables or disables automatic selection of any idle appearance for transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Optional Boolean Communication Manager selects the first idle appearance. coverageMsgRetrieval	Optional	Boolean
coverageMsgRetrieval	Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.	Optional	Boolean
autoAnswer	In EAS environments, the auto answer setting	Optional	Valid entries: 1. all: All ACD and non-ACD calls

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	for the Agent LoginID can override a endpoint's setting when an agent logs in.		ended to an idle endpoint cut through immediately. Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when the Allow Ringer-off with Auto-Answer is enabled for the system. 2. acd: Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls ended to a endpoint ring audibly. For analog endpoints, the endpoint is off-hook and idle, only the ACD split/skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the endpoint is active on an ACD call and a

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			non-ACD call arrives, the Agent receives call-waiting tone. 3. none: All calls ended to this endpoint receive an audible ringing treatment. 4. icom: Allows a telephone user to answer an intercom call from the same intercom group without pressing the intercom button.
dataRestriction	Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if Auto Answer is administered as all or acd. If enabled, whisper page to this endpoint is denied.	Optional	
idleAppearancePreference	Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.	Optional	true - The user connects to an idle call appearance instead of the ringing call. false - The Alerting Appearance

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			Preference is set and the user connects to the ringing call appearance.
callWaitingIndication	enable/disable call waiting for this endpoint	Optional	
attCallWaitingIndication	Attendant call waiting allows attendantoriginated or attendant-extended calls to a busy single-line telephone to wait and sends distinctive call-waiting tone to the single-line user. Enable/disable attendant call waiting	Optional	Boolean
distinctiveAudibleAlert	Enter true so the telephone can receive the 3 different types of ringing patterns which identify the type of incoming calls. Distinctive ringing might not work properly for off-premises telephones.	Optional	
restrictLastAppearance		Optional	Valid entries: 1. true: Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only. 2. false: Last idle call appearance is used for incoming priority

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			calls and outgoing call originations.
adjunctSupervision	Enable / Disable adjunct Supervision.	Optional	Valid entries: 1. true: Analog disconnect signal is sent automatically to the port after a call ends. Analog devices (such as answering machines and speakerphones) use this signal to turn the devices off after a call ends. 2. false: Hunt group agents are alerted to incoming calls. In a hunt group environment, the disconnect signal blocks the reception of zip tone and incoming call notification by an auto-answer endpoint when a call is queued for the endpoint.
perStationCpnSendCallingNumber	Send Calling Number.	Optional	Valid entries: 1. y: All outgoing calls from the endpoint will deliver the Calling Party Number (CPN) information as

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			"Presentation Allowed." 2. n: No CPN information is sent for the call 3. r: Outgoing non-DCS network calls from the endpoint will deliver the Calling Party Number information as "Presentation Restricted."
busyAutoCallbackWithoutFlash	Appears on the Endpoint screen for analog telephones, only if the Without Flash field in the ANALOG BUSY AUTO CALLBACK section of the Feature-Related System Parameters screen is set to true. The Busy Auto Callback without Flash field then defaults to true for all analog telephones that allow Analog Automatic Callback. Set true to provide automatic callback for a calling analog endpoint without flashing the hook.	Optional	
audibleMessageWaiting	Provides audible message waiting	Optional	Boolean
displayClientRedirection	Only administrable if Hospitality is enabled on the System Parameters Customer- Options	Optional	Boolean

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	(Optional Features) screen. This field affects the telephone display on calls that originated from a endpoint with Client Room Class of Service. Note: For endpoints with an audix endpoint type, AUDIX Voice Power ports, or ports for any other type of messaging that needs display information, Display Client Redirection must be enabled. Set true to redirect information for a call originating from a Client Room and ending to this endpoint displays.		
selectLastUsedAppearance		Optional	Valid entries: 1. True: Indicates that a endpoint's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. If you enter true, the line selection on an on-hook endpoint only moves from the last used line button to a line button with an audibly alerting call. If there are no alerting calls,

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			the line selection remains on the button last used for a call. 2. false: The line selection on an on-hook endpoint with no alerting calls can be moved to a different line button, which might be serving a different extension.
coverageAfterForwarding	Whether an unanswered forwarded call is provided coverage treatment.	Optional	
directIpIpAudioConnections	Allow/disallow direct audio connections between IP endpoints.	Optional	
ipAudioHairpinning	Allows IP endpoints to be connected through the server's IP circuit pack.	Optional	
primeAppearancePreference	Set prime appearance preference.	Optional	
endpointSiteData	This is complex type for Site Data fields		
room	This is field of Site Data	Optional	Max length 10
jack	This is field of Site Data	Optional	Max length 5
cable	This is field of Site Data	Optional	Max length 5
floor	This is field of Site Data	Optional	

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
building	This is field of Site Data	Optional	
headset	This is field of Site Data	Optional	
speaker	This is field of Site Data	Optional	
mounting	This is field of Site Data	Optional	Valid values d, w.
cordLength	This is field of Site Data	Optional	Valid range from 0 to 99.
setColor	This is field of Site Data	Optional	
abbrList	This is complex type for Station Abbreviated Dialing Data fields.	Optional	
listType	This is field of Station Abbreviated Dialing Data.	Mandatory	Valid values enhanced, group, personal, system.
number	This is field of Station Abbreviated Dialing Data.	Mandatory	A number.
buttons	This is complex type for button data	Optional	
Number	This is field of button data.	Mandatory	
Type	This is field of button data.	Optional	
data1	This is field of button data.	Optional	
data2	This is field of button data.	Optional	
data3	This is field of button data.	Optional	
data4	This is field of button data.	Optional	
data5	This is field of button data.	Optional	

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
data6	This is field of button data.	Optional	
endpointDataModule	This is complex type for Station Data module.	Optional	
dataExtension	This is field of Station Data module.	Mandatory	
name	This is field of Station Data module.	Optional	Max length 29
Class of restriction cor	This is field of Station Data module.	Mandatory	Valid range from 0 to 995.
Class of Service Cos	This is field of Station Data module.	Mandatory	Valid range from 0 to 15.
itc	This is field of Station Data module.	Mandatory	Valid values: 1. restricted 2. unrestricted
Tenant Number	This is field of Station Data module.	Mandatory	Valid range from 1 to 100.
listType	This is field of Station Data module.	Optional	Valid values: 1. enhanced 2. group 3. personal 4. system
listId	This is field of Station Data module.	Optional	
specialDialingOption	This is field of Station Data module.	Optional	Valid values: 1. default 2. hot-line
specialDialingAbbrDialCode	This is field of Station Data module.	Optional	
hotLineDestAbbrevList	This is field of Station Hot Line Data.	Optional	Valid range 1 to 3
hotLineAbbrevDialCode	This is field of Station Hot Line Data.	Optional	Numeric string

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
nativeName	This is complex type of Native Name Data.	Optional	
locale	This is field of Native Name Data. **Note:** If the **displayName**, **givenName**, or **surname** contains characters of multiple scripts then the locale tag should be present. The locale for the multiscript languages are: • Japanese: **ja** • Simplified Chinese: **zh-cn** • Traditional Chinese: **zh-tw** • Korean: **ko-kr** • Vietnamese: **vi-vn** The locale tag is case sensitive.	Optional	
Name	This is field of Native Name Data.	Mandatory	Max length 27

Attribute details defined in the Messaging communication profile XSD

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
Messaging System Name messagingName	Name of Messaging System	Mandatory	
Use Existing Mailbox number	'true' if already created mailbox	Optional	

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
useExisting	number is to be used. 'false' if available mailbox number is to be used.		
Messaging Template messagingTemplate	Specifies the messaging template of a subscriber.	Optional	
Password password	Specifies the default password the subscriber must use to log in to his or her mailbox.	Mandatory	The password can be from one digit in length to a maximum of 15 digits.
deleteOnUnassign		Optional	
Class of service cos	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size.	Optional	Valid ranges from 0 to 995
Community ID communityID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers.	Optional	The default value is 1.
Email Handle emailHandle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.	Optional	

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
Common Name commonName	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications.	Optional	The name you enter can be 1 to 64 characters in length.
secondaryExtension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.	Optional	Valid values 0 to 9 number values of length 10
mmSpecific	This is complex type for Messaging specific fields data.	Optional	
numericAddress	This is field of Messaging specific data. Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.	Optional	
pbxExtension	This is field of Messaging specific data. The primary telephone extension of the subscriber.	Optional	
telephoneNumber	This is field of Messaging specific data.	Optional	The entry can be a maximum of 50 characters in length

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
	The telephone number of the subscriber as displayed in address book listings and client applications.		and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]).
asciiVersionOfName	This is field of Messaging specific data. If the subscriber name is entered in multibyte character format, then this field specifies the ASCII translation of the subscriber name.	Optional	
expirePassword	This is field of Messaging specific data. Specifies whether your password expires or not.	Optional	You can choose one of the following: • yes: for password to expire • no: if you do not want your password to expire
mailBoxLocked	This is field of Messaging specific data. Specifies whether you want your mailbox to be locked. A subscriber mailbox can become locked after two unsuccessful login attempts.	Optional	You can choose one of the following: • no: to unlock your mailbox • yes: to lock your mailbox and prevent access to it
personalOperatorMailbox	This is field of Messaging specific data. Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the	Optional	

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
	transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.		
personalOperatorSchedule	This is field of Messaging specific data. Specifies when to route calls to the backup operator mailbox. The default value for this field is Always Active.	Optional	
tuiMessageOrder	This is field of Messaging specific data. Specifies the order in which the subscriber hears the voice messages.	Optional	You can choose one of the following: • urgent first then newest: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • oldest messages first: to direct the system to play messages in the order they were received. • urgent first then oldest: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
			urgent messages are played in the order of how they were received. • newest messages first: to direct the system to play messages in the reverse order of how they were received.
intercomPaging	This is field of Messaging specific data. Specifies the intercom paging settings for a subscriber.	Optional	You can choose one of the following: • paging is off: to disable intercom paging for this subscriber. • paging is manual: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • paging is automatic: if the TUI automatically allows callers to page the subscriber.
voiceMailEnabled	This is field of Messaging specific data. Specifies whether a subscriber can receive messages, e-mail messages and callanswer messages from other subscribers. You can choose one of the following: - yes: to allow the subscriber	Optional	

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
	to create, forward, and receive messages. - no: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.		
miscellaneous1	This is field of Messaging specific data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.		Max length 51
miscellaneous2	This is field of Messaging specific data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.		Max length 51
miscellaneous3	This is field of Messaging specific data. Specifies additional, useful information about a subscriber. Entries in this field		Max length 51

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
	are for convenience and are not used by the messaging system.		
miscellaneous4	This is field of Messaging specific data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.		Max length 51
cmmSpecific	This is field of Messaging specific data. Specifies the number of the switch on which this subscriber's extension is administered.	Optional	You can enter "0" through "99", or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.
accountCode	This is field of CMM data. Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you	Optional	

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
	enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.		
coveringExtension	This is field of CMM data. Specifies the number to be used as the default destination for the Transfer Out of Messaging feature.	Optional	You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.
miscellaneous1	This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11
Miscellaneous2	This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11
Miscellaneous2	This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by	Optional	Max length 11

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
	the messaging system.		
Miscellaneous4	This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11

Attribute details defined in the Session Manager communication profile XSD

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
Primary Session Manager primarySM	Specify the name of the Session Manager instance that must be used as the home server for a Communication Profile. As a home server, the primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network.	Mandatory	
Secondary Session Manager secondarySM	If a secondary Session Manager instance is specified, this Session Manager provides continued service to SIP devices associated with this Communication	Optional	

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
	Profile in the event that the primary Session Manager is not available.		
Origination Application Sequence originationAppSequence	Specify an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. **Note:** If an origination and a termination application sequences are specified, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.	Optional	
Termination Application Sequence terminationAppSequence	Specify an Application Sequence that will be invoked when calls are routed to this user. A selection is optional. **Note:** If an origination and a termination application sequences are specified, and if each sequence contains a Communication Manager application, Communication	Optional	

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
	Manager must be the same in both the sequences.		
Survivability Server survivabilityServer	For local survivability, the name of a Survivability Server (a SIP Entity) can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is specified, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager.	Optional	
Home Location homeLocation	Specify a Home Location (the name of a Location –	Mandatory	

Attribute	Attribute Description	Mandator y/ Optional	Validation Constraints
	navigate to Routing > Locations) to support mobility for a user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this “home” location regardless of the physical location of the SIP device used to make the call. A selection is mandatory.		

Import Users field descriptions

Use this page to bulk import users and their attributes from a valid XML file.

File Selection

Name	Description
Select File	The path and name of the XML file from which you import the users.

Button	Description
Browse	Opens a dialog box that you can use to select the file from which you import the users.

General

Name	Description
Select Error Configuration	The options are: • **Abort on first error**. Aborts importing the user records when the import user

Name	Description
	operation encounters the first error in the import file containing the user records. • **Continue processing other records**. Imports the next user record even if the import user operation encounters an error while importing a user record.
Select Import Type	The options are: • **Complete**. Imports users with all the user attributes. • **Partial**. Imports users with specific user attributes.
If a matching record already exists	The options are: • **Skip**. Skips a matching user record that already exists in the system during an import operation. Currently, with this option you can add a new communication profile to a communication profile set but you cannot update an existing communication profile in a communication profile set. **Note:** This option is not available if you select the **Partial** option in **Select Import Type**. • **Replace**. Re-imports or replaces all the data for a user including access control lists, contact lists, and so on. With this option, you can replace a user and the associated data of the user. • **Merge**. Imports the user data at an even greater degree of granularity. Using this option you can simultaneously perform both add and update operation of users. For example, add a contact to a contact list and update a last name. • **Delete**. Deletes the user records from the database that match the records in the input XML file. **Note:** The system confirms that a user already exists in the database by matching the login name of the user in the database

Name	Description
	with the login name of the user in the imported file.

Job Schedule

Name	Description
Schedule Job	The options for configuring the schedule of the job: • **Run immediately**. Use this option to run the import job immediately. • **Schedule later**. Use this option to run the job at the specified date and time.
Date	The date on which you run the import users job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.
Time	The time of running the import users job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format. This field is available when you select the **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Button	Description
Import	Imports or schedules the import operation based on the option you selected.

Manage Job

Name	Description
Select check box	Use this check box to select a job.
Scheduled Time	The time and date of scheduling the job.
Status	The current status of the job. The following are the different status of a job: 1. PENDING EXECUTION. The job is in queue. 2. RUNNING. The job execution is in progress.

Name	Description
	3. SUCCESSFUL. The job execution is completed. 4. INTERRUPTED. The job execution is cancelled. 5. PARTIAL FAILURE. The job execution has partially failed. 6. FAILED. The job execution has failed.
Job Name	A link to the Scheduler user interface. You can cancel the job from the Scheduler user interface too.
% Complete	The job completion status in percentage.
User Records	The total user records in the input file.
Warnings	Number of user records in the input file with warnings.
Errors	Number of user records in the input file that failed to import.

Button	Description
View Job	Shows the details of the selected job.
Cancel Job	Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.
Delete Job	Deletes the selected job.
Refresh	Refreshes the job information in the table.
Show	Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select **All** to view all the jobs on a single page.
Select: All	Selects all the jobs in the table.
Select: None	Clears the check box selections.
Previous	Displays jobs in the previous page.
Next	Displays jobs in the next page.
Done	Takes you back to the **User Management** page.

Import Users – Job Details field descriptions

The Import Users-Job Details page displays the details of the selected job.

Name	Description
Name	Displays the import job that the end user initiates.
Scheduled by	Displays the name of the user who initiates or schedules the import job
Scheduled at	Displays the start time of the import job.
Error Configuration	Displays the value that was configured for error while scheduling the Import Job. The possible values for this field are **Abort on first error** and **Continue processing other records**.
Import Type	Displays the value configured for the **Import Type** field while scheduling the import job. Possible values are **Complete** and **Partial**.
Import Option	Displays the value that was configured for the **If a matching record already exists** field while scheduling the import job. The possible values for this field are **Skip**, **Merge**, **Replace**, and **Delete**.
End	Displays the end date and time of the job.
Status	Displays the status of the job.
File	Displays the name of the file that is used to import the user records.
Count	Displays the total number of user records in the input file.
Success	Displays the total number of user records that are successfully imported.
Fail	Displays the total number of user records that failed to import.
Warning	Displays the total number of user records that successfully imported, however, there are warnings generated for the user records.
Message	Displays a message that indicates whether the import is successful or failure.

Name	Description
Completed	Displays the percentage completion of the import.

Name	Description
Line Number	Displays the line number in the file where the error occurred.
Login Name	Displays the login name of the user record that failed to be imported.
Error Message	Displays a brief description of the error.

Button	Description
Download	Exports and saves the user import error records in an XML file to the specified destination. **Note:** This button is not available if there are no error records for user Import Jobs or if the import job type is set to **Abort on first error**.
Cancel	Takes you back to the Import Users page.

To enable the **Download** button, on the User bulk import configuration page, set the **Enable Error File Generation** attribute to **True**.

To navigate to the User bulk import configuration page from the System Manager console, click **Services** > **Configurations** > **Settings** > **SMGR** > **User BulkImport profile**.

Import Global Settings field descriptions

Use this page to bulk import shared addresses, public contacts, and presence access control list (ACLs) records from a valid XML file. These imported items are also called global user settings.

File Selection

Name	Description
Select File	The path and name of the XML file from which you want to import the global settings records.

Button	Description
Browse	Opens a dialog box that you can use to select the file from which you want to import the global user settings.

General

Name	Description
Select Error Configuration	The options are: • **Abort on first error**: Aborts importing the global user settings records when User Management encounters the first error in the import file containing the global user settings records. • **Continue processing other records**: Imports the next global user settings record even if User Management encounters an error while importing a global user settings record.
If a matching record already exists	The options are: • **Skip**: Skips a matching global user settings record that already exists in the system database during an import operation. Currently, using this option you can add a new public contact to a public contact set but you cannot update an existing public contact in a public contact set. • **Replace**: Re-imports or replaces all the global user setting records in the import file. This is essentially the ability to replace a user along with the other data related to the global user settings. • **Merge**: Imports the global user settings data at an even greater degree of granularity. For example, add a shared address to a shared address list or update a public contact. • **Delete**: Deletes the global setting records from the database that matches the records in the input XML file.

Job Schedule

Name	Description
Schedule Job	The settings for configuring the schedule of the job: • **Run immediately**: Use this option if you want to run the import job immediately. • **Schedule later**: Use this option to run the job at the specified date and time.
Date	The date when you want to run the import job. The date format is mm dd yyyy. You can use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.
Time	The time of running the import job. The time format is hh:mm:ss and 12 (AM or PM) or 24–hour format. This field is available when you select the **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Button	Description
Import	Imports or schedules the import operation based on the option you selected.

Manage Job

Name	Description
Select check box	Use this check box to select a job.
Scheduled Time	The date and time when job was scheduled.
Status	The current status of the job. The following are the different status of a job: 1. PENDING EXECUTION: The job is in queue. 2. RUNNING: The job execution is in progress. 3. SUCCESSFUL: The job execution is completed.

Name	Description
	4. INTERRUPTED: The job execution is cancelled. 5. PARTIAL FAILURE: The job execution has partially failed. 6. FAILED: The job execution has failed.
Job Name	A link to the Scheduler user interface. You can cancel the job from the Scheduler user interface too.
% Complete	The job completion status in percentage.
Records	The total number of global user settings records in the input file.
Error	The number of global user settings records in the input file that failed to import.

Button	Description
View Job	Shows the details of the selected job.
Cancel Job	Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.
Delete Job	Deletes the selected job.
Refresh	Refreshes the job information in the table.
Show	Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select **All** to view all the jobs on a single page.
Select: All	Selects all the jobs in the table.
Select: None	Clears the check box selections.
Previous	Displays jobs in the previous page.
Next	Displays jobs in the next page.
Done	Takes you back to the **User Management** page.
Cancel	Cancels the import operation and takes you back to the User Management page.

Job Details field descriptions

The Job Details page displays the details of the selected Job.

Name	Description
Name	Specifies the name of the import job.
Scheduled by	Name of the user who initiated or scheduled the import job.
Scheduled at	Start time of the scheduled job.
End	End date and time of the job.
Status	Status of the job.
File	Name of the file that is used to import the global user settings records.
Count	Total number of global user settings records in the input file.
Success	Total number of global user settings records that are successfully imported.
Fail	Total number of global user settings records that failed to import.
Message	The message that indicates whether the import is successful or failure.
Completed	Displays the percentage completion of the import.

Name	Description
Record Number	Failed XML element in the input XML file.
Name	Name of the failed XML element.
Error Message	A brief description of the error.

Button	Description
Cancel	Takes you back to the Import Users page.

Quick start to importing users

Quick start to importing users

This section describes how to quickly create an XML file for importing users in bulk. This XML file includes user profiles with core attributes as well as with SIP phone (SIP communication profile).

XML for user with core attributes

Following are the minimal elements for mapping the user import XML with user interface fields:

Table 3: Minimal elements

UI field	Description	XML tag	Possible value
Authentication Type	Specifies the type of authentication.	`<authenticationType>` ... `</authenticationType>` >	Basic or Enterprise
First Name	Specifies the first name of the user.	`<givenName>` ... `</givenName>`	First name of the user.
Login Name	Specifies the primary handle of user.	`<loginName>` ... `</loginName>`	User log-in name.
Last Name	Specifies the last name of the user.	`<surname>` ... `</surname>`	Last name of the user.
Login Password	Specifies the password used to log in to System Manager.	`<userPassword>` ... `</userPassword>`	Log-in password of the user.

Sample XML with a single user profile

The following sample XML contains a user profile with basic fields. To create your own XML, replace the value of the tags explained in the Minimal elements table in *XML for user with core attributes*.

```
<?xml version="1.0" encoding="UTF-8"?>
    <!--  Root Element 'Users' represent collection of  user (containing 1 or more
users)-->
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"  xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/
schema/import userimport.xsd" >

  <tns:user>
    <authenticationType>Basic</authenticationType>
    <givenName>John</givenName>
    <loginName>jmiller@avaya.com</loginName>
    <surname>Miller</surname>
    <userPassword>mypassword</userPassword>
  </tns:user>
</tns:users>
```

The highlighted XML tag in the user profile XML represents the data for a single user tag that starts and ends with `</tns:user>`. To create multiple users in the same XML, repeat the highlighted content multiple times with different user values.

For example, the following sample XML contains two users, John Miller and Roger Philip. Note that there are two instances of the `<tns:user>` tag, one for each user.

```
<?xml version="1.0" encoding="UTF-8"?>
    <!--  Root Element 'Users' represent collection of  user (containing 1 or more
users)-->
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"  xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/
schema/import userimport.xsd" >

  <tns:user>
    <authentication>TypeBasic</authenticationType>
    <givenName>John</givenName>
    <loginName>jmiller@avaya.com</loginName>
    <surname>Miller</surname>
    <userPassword>mypassword</userPassword>
  </tns:user>

<tns:user>
    <authenticationType>Basic</authenticationType>
    <givenName>Roger</givenName>
    <loginName>rphilip@avaya.com</loginName>
    <surname>Philip</surname>
    <userPassword>mypassword</userPassword>
  </tns:user>

</tns:users>
```

Note:

The XML is a text file. Therefore, you can edit this XML in any text editor.

Related topics:

XML for user with core attributes on page 289

Bulk import XML for users with SIP phone

To create a user XML, first perform the procedure for bulk importing users in the *Bulk importing users* section. If communication address is added to the user, then the **commPassword** field is mandatory.

To assign communication address, the mapping of Communication Profile for a new SIP user is as follows:

Table 4: Mapping of Communication Profile for a new SIP user

UI field	Description	XML tag	Possible value

Name	Specifies the name of the communication profile.	`<commProfileSetName>`
		...
		`</commProfileSetName>`
			The unique name of this communication profile.

UI field	Description	XML tag	Possible value

Default	Indicates whether this is a default profile.	`<isPrimary>`
		...
		`</isPrimary>`
			True or False.

The attributes to set up the communication address for a user are as follows:

Table 5: User attributes to set up communication address

UI field	Description	XML tag	Possible value

Handle	Specifies the extension number of the user.	`<handleName>`
		...
		`</handleName>`
			Extension number.

Type	Specifies the communication type of the user profile.	`<handleType>`
		...
		`</handleType>`
			Communication type. For example, sip and smtp.

SubType	Specifies the communication subtype of the user profile.	`<handleSubType>`
		...
		`</handleSubType>`
			Communication sub type. For example, username, e164, and msrtc.

Domain	Specifies the domain name of the user.	`<domainName>`
		...
		`</domainName>`
			Name of the configured SIP domain name.

The following is the mapping of SIP Manager Communication Profile elements with the corresponding user interface fields.

Table 6: Mapping of SIP Manager Communication Profile elements

UI field	Description	XML tag	Possible value

Primary Session Manager	Specifies the name of the primary Session Manager instance that is used as the home server for a communication profile.	`<sm:primarySM>`
		...
		`</sm:primarySM>`
		>
			Enter the name of Session Manager.

Origination Application Sequence	Specifies the Application Sequence that is invoked when calls are routed from this user.	`<sm:originationAppSequence>`
		...
		`</sm:originationAppSequence>`
			True or False.

UI field	Description	XML tag	Possible value

Termination Application Sequence	Specifies the Application Sequence that is invoked when calls are routed to this user.	`<sm:terminationAppSequence>`
		...
		`</sm:terminationAppSequence>`	

Home Location	Specifies the routing home location.	`<sm:homeLocation>`
		...
		`</sm:homeLocation>`	

The following is the mapping of CM Endpoint Profile elements with the corresponding user interface fields.

Table 7: Mapping of CM Endpoint Profile elements

UI field	Description	XML tag	Possible value

System	Specifies the SIP Entity of the Communication Manager.	`<ipt:cmName>`
		...
		`</ipt:cmName>`
			Name of the configured Communication Manager.

Use Existing	Indicates whether the station is already defined in the system.	`<ipt:useExistingExtension>`
		...
		`</ipt:useExistingExtension>`
			True or False.

Extension	Specifies the extension number for this profile.	`<ipt:extension>`
		...
		`</ipt:extension>`	

Template	Specifies the template name used for creating the station.	`<ipt:template>`
		...
		`</ipt:template>`	

Set Type	Specifies the set type of the station.	`<ipt:setType>`
		...
		`</ipt:setType>`	

Port	Specifies the port number from the list for the template you select.	`<ipt:port>`
		...
		`</ipt:port>`	

Related topics:

Bulk importing of users on page 106

Sample XML file for a user with SIP Communication Profile

Here is the sample XML of a user profile with basic fields. To create your own XML, replace the value of the tags explained in the Mapping of CM Endpoint Profile elements table in *Bulk import XML for users with SIP phone*.

```
<?xml version="1.0" encoding="UTF-8"?>
    <!--  Root Element 'Users' represent collection of  user (containing 1 or more
users)--
tns:users xmlns:tns="http://xml.avaya.com/schema/import"  xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/
schema/import userimport.xsd" >
    <tns:user>
    <authenticationType>BASIC</authenticationType>
    <givenName>John</givenName>
    <loginName>jmiller@avaya.com</loginName>
    <surname>Miller</surname>
    <userPassword>mypassword</userPassword>
    <commPassword>12345</commPassword>
      <commProfileSet>
      <commProfileSetName>Primary</commProfileSetName>
      <isPrimary>true</isPrimary>
      <handleList>
        <handle>
          <handleName>sip:jmiller@avaya.com</handleName>
          <handleType>sip</handleType>
          <handleSubType>msrtc</handleSubType>
        </handle>
       </handleList>
      <!--The below is extended communication profile-->
      <commProfileList>
          <commProfile xsi:type="sm:SessionManagerCommProfXML" xmlns:sm="http://
xml.avaya.com/schema/import_sessionmanager">
            <commProfileType>SessionManager</commProfileType>
            <sm:primarySM>IBM1-Performance</sm:primarySM>
            <sm:terminationAppSequence>Perf_CM_Appl_Seq</sm:terminationAppSequence
            <sm:originationAppSequence>Perf_CM_Appl_Seq</sm:originationAppSequence
            <sm:homeLocation>SIT Lab</sm:homeLocation>
          </commProfile>

          <commProfile xsi:type="ipt:xmlStationProfile" xmlns:ipt="http://
xml.avaya.com/schema/import_csm_cm">
            <commProfileType>CM</commProfileType>
            <ipt:cmName>Performance_CM</ipt:cmName>
            <ipt:useExistingExtension>false</ipt:useExistingExtension>
            <ipt:extension>28000</ipt:extension>
            <ipt:template>DEFAULT_9620SIP_CM_5_2</ipt:template>
            <ipt:setType>9620SIP</ipt:setType>
            <ipt:port>S08012</ipt:port>
          </commProfile>
        </commProfileList>

      </commProfileSet>
    </tns:user>
</tns:users>
```

Related topics:

Bulk import XML for users with SIP phone on page 290

Managing communication profiles

Communication profiles

Using the Users feature, you can provide communication profiles to associate elements with users. Communication Profiles supports communication interactions established through Avaya Communication Services. Communication Profiles can be Endpoint, Messaging, Session Manager, CS1000, CallPilot Messaging, MMCS Conferencing, or B5800 Branch Gateway Endpoint Profile.

You can provide Communication Profiles in UPM through Communication Profile Extension Pack (EP). You can use a communication profile to represent a subscription of the user to a communication subsystem and the specific configuration needs for the user. A communication subsystem is a service or infrastructure that manages the establishment and controls or routes the communication interactions.

Creating a new communication profile

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a new user account, click **New**.
   - To add a communication profile to an existing user, select the user and click **Edit**.
4. On the New User Profile or the User Profile Edit page, click the **Communication Profile** tab.
5. In the communication profile section, click **New**.
6. In the **Name** field, enter the name of the new communication profile.
7. To mark the profile as default, select the **Default** check box.
8. Click **Done**.
9. Click **Commit**.

Related topics:

New User Profile field descriptions on page 361

Deleting a communication profile

About this task

You cannot delete default communication profiles.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. Perform one of the following steps:
   - On the User Management page, select a user and click **Edit**.
   - On the User Management page, select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Communication Profile section, click a profile.
6. Click **Delete**.
7. Click **Commit**.

Result

When you delete a communication profile, System Manager deletes all the communication addresses associated with the communication profile.

Creating a new communication address for a communication profile

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a new user account, click **New**.
   - To add a communication profile address to an existing user, select the user and click **Edit**.
4. On the New User Profile or the User Profile Edit page, click the **Communication Profile** tab.
5. In the Communication Profile section, click a communication profile.
6. In the Communication Address section, click **New**.
7. In the **Type** field, enter a communication protocol.

8. In the **Fully Qualified Address** field, enter a contact address in the format supported by the value that you selected in the **Type** field. A contact address can be an e-mail ID, instant messenger ID, or the SIP address of a SIP-enabled device.
9. Enter the domain name from the field next to **Fully Qualified Address** field.
10. Click **Add**.
11. Click **Commit**.

Related topics:

User Profile Edit field descriptions on page 346
New User Profile field descriptions on page 361

Modifying a communication address of a communication profile

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. Perform one of the following steps:
   - On the User Management page, select a user and click **Edit**.
   - On the User Management page, select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Communication Profile section, select a profile.
6. In the Communication Address section, select a communication address.
7. Click **Edit**.
8. Modify the information in the respective fields.
9. Click **Add**.
10. Click **Commit**.

Related topics:

User Profile Edit field descriptions on page 346
New User Profile field descriptions on page 361

Deleting a communication address from a communication profile

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following:
   - Select a user and click **Edit**.
   - Select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Communication Profile section, click a communication profile.
6. In the Communication Address section, select a communication address from the table.
7. Click **Delete**.
8. Click **Commit**.

Related topics:

User Profile Edit field descriptions on page 346
New User Profile field descriptions on page 361

Session Manager Communication profile administration

The Session Manager Profile sub-section of the Communication Profile section enables associating a primary Session Manager instance as a home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network.

All Communication Addresses (handles) of type SIP for the Communication Profile will be associated with the Aura network. If a secondary Session Manager instance has been selected, it will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available.

Application Sequences may be specified to be invoked when routing calls from (origination application sequence) or to (termination application sequence) the currently displayed user.

A Conference Factory Set can be specified for users for experiencing improved voice, video and text conferencing.

For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session

Manager is selected, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application will continue locally to the Communication Manager LSP resident with the Branch Session Manager.

When this user calls numbers that are not associated with an administered user, dial-plan rules are applied to complete the call based on this home location if the IP address of the SIP device used to make the call has not been assigned to a location.

CM Endpoint Profile Administration

CM Endpoint and Messaging profiles of a user

With User Profile Management, you can create the following types of communication profiles for a user:

- CM Endpoint Profile, to create an association between an endpoint and a user
- Messaging Profile, to create an association between a subscriber mailbox and a user

You can add, view, modify, and delete endpoint and messaging profiles. You can go to Endpoint or Subscriber Management pages to modify any of the endpoint or subscriber fields that are not available through User Profile Management.

Login name of endpoint or messaging profile

The login name in the Identity section on the New User Profile and Edit User Profile pages is the user name that is associated with the communication profile, CM Endpoint and Messaging. This user name appears in the User column in the Endpoint List or Subscriber List.

For endpoints, the **Localized Display Name** and **Endpoint Display Name** fields in the Identity section of the User Profile Management user profile map to the **Name** and **Native Name** fields of CM Endpoint. The **Localized Display Name** and **Endpoint Display Name** fields are optional. They default to the **Last Name** and **First Name** as given in the General section of the User Profile Management user profile. You can also fill in any other name of your choice.

For Subscribers, the **Last Name** and **First Name** fields in the General section of User Profile Management user profile directly map to the **Last Name** and **First Name** fields in Subscriber. The **Localized Display Name** and **Endpoint Display Name** fields are not applicable for Subscribers.

Creating CM Endpoint and Messaging profiles

You can create one default or primary Communication Profile for a user. To this default profile, you can add one CM Endpoint and one Messaging profile. In addition, you can add two more CM Endpoint profiles. You can add a maximum of three CM Endpoint profiles and one Messaging profile per user.

Adding a CM Endpoint profile for a user

Before you begin

Add Communication Manager using Runtime Topology System (RTS).

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.

2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - If you are creating a CM Endpoint profile for a new user profile, click **New**.
   - If you are creating a CM Endpoint profile for an existing user, select the user and click **Edit**.
4. Click the **Communication Profile** tab.
5. In the CM Endpoint Profile section, select the check box next to the **CM Endpoint Profile** label.
6. In the CM Endpoint Profile section, enter the relevant information.

   Note:

   To delete the endpoint from the communication management device after removing the association between the endpoint and the user, select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box.
7. Perform one of the following procedures:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page for making further modifications, **Commit & Continue**.

   From User Management, you can create or add endpoints. After you select the Communication Manager in which you want to add an endpoint, the system allows you to complete the fields for creating a new endpoint.

   The **Preferred Handle** field specifies numeric only handles, SIP or non SIP, that are administered for a user. If the SIP entity is of Communication Manager type, Session Manager uses the **Preferred Handle** field in the CM Endpoint profile. By default, for a SIP station, Communication Manager uses the extension number as the phone number entry on an OPS station-mapping table. If your enterprise dial plan has SIP handles that are different from the Communication Manager extension, then use the **Preferred Handle** field to change the phone number entry on the OPS station-mapping table on the Communication Manager.

   To modify the phone number entry, the Communication Address in System Manager should have a SIP handle. In the CM Endpoint Communication Profile, set the **Preferred Handle** field to the SIP handle format. After you click **Commit**, System Manager sets the **Phone Number** field in the OPS station-mapping table on Communication Manager to the SIP handle format. If you do not need this feature then set the **Preferred Handle** value to **None**.

Related topics:

New User Profile field descriptions on page 361

Viewing a station profile of a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. Click the **Communication Profile** tab.

Modifying a CM Endpoint profile of a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the CM Endpoint Profile section, modify the relevant information in the fields.
6. To save the changes to the database, click **Commit**.
   To cancel the action and return to the previous page, click **Cancel**.

Related topics:

New User Profile field descriptions on page 361

Removing association between an CM Endpoint and a user

Before you begin

Ensure that you have not selected the **Delete Endpoint on Unassign of Endpoint from User or Delete User** check box while associating a station with a user.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.

4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
6. Click **Commit**.

Result

The system removes the association between the endpoint and the user. The endpoint is still provisioned on the communication management device.

Deleting an CM Endpoint profile of a user

Before you begin

You have selected the **Delete Endpoint on Unassign of Endpoint from User or Delete User** check box while associating a endpoint to a user.

About this task

The delete functionality removes the association between the endpoint and the user, and deletes the endpoint from the communication management device.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
6. Click **Commit**.

Note:

You can delete only those endpoints that are associated with a user through User Management. You can delete non-user associated endpoints through Endpoint management.

Related topics:

New User Profile field descriptions on page 361

Messaging Profile Administration

Adding a messaging profile for a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - If you are creating a messaging profile for a new user profile, click **New**.
   - If you are creating a messaging profile for an existing user, select the user and click **Edit**.
4. Click the **Communication Profile** tab.
5. In the Messaging Profile section, select the check box next to the **Messaging Profile** label.
6. In the Messaging Profile section, complete the relevant fields.

   Note:

   To delete the subscriber mailbox from the communication management device after removing the association between the subscriber and the user, select the **Delete Messaging on Unassign of Subscriber from User or Delete User** check box.

7. Click **Commit** or **Commit & Continue** to add the messaging profile, or click **Cancel** to return to return to the previous page.

   The field names that are marked with an asterisk (*) are mandatory fields. You must enter valid information in these fields to create the CM Endpoint profile.

   Note:

   You must add the messaging devices through Runtime Topology System (RTS) before you add a messaging profile for a user. After you create the user-subscriber association, the user name appears in the **User** column in the subscriber list.

Related topics:

New User Profile field descriptions on page 361

Modifying a messaging profile of a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.

2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile section, modify the relevant information in the fields.
6. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Related topics:

New User Profile field descriptions on page 361

Viewing a messaging profile of a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. Click the **Communication Profile** tab.

Result

The Messaging Profile section displays the messaging profile information of the user.

Related topics:

New User Profile field descriptions on page 361

Removing association between a subscriber mailbox and a user

Before you begin

The **Delete Subscriber on Unassign of Subscriber from User or Delete User** check box is clear while associating a mailbox with a user.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile tab, clear the check box next to the **Messaging Profile** label.
6. Click **Commit**.

Result

The system removes the association between the subscriber mailbox and the user. The subscriber mailbox is still provisioned on the communication management device.

Deleting a subscriber mailbox

Before you begin

You have selected the **Delete Subscriber on Unassign of Subscriber from User or on Delete User** check box while associating a subscriber mailbox to a user.

About this task

This functionality deletes the subscriber mailbox from the messaging device after removing the association between the subscriber mailbox and the user.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile section, clear the check box next to the **Messaging Profile** label.
6. Click **Commit**.

Note:

You can delete only those subscribers that are associated with a user through User Management. You can delete non-user associated subscriber mailboxes only through Subscriber Management.

CS 1000 and CallPilot profile administration

CS 1000 and CallPilot profile administration

With User Management, you can create the following types of communication profiles for a user:

- CS 1000 Endpoint Profile. To create an association between an endpoint and a user.
- CallPilot Messaging Profile. To create an association between a subscriber mailbox and a user.

To modify an endpoint or subscriber field that is not available through User Management, navigate to the Endpoint or Subscriber Management pages and modify the information. For information, see Redirecting the or user to Element Manager on page 305.

Redirecting the CS 1000 or CallPilot user to Element Manager

Before you begin

A user must exist with at least one communication profile. To create a user, navigate to **User Management** > **New**.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the CS 1000 Endpoint Profile or CallPilot Messaging Profile section you want to update, click **Update**.

   The system opens the user profile in the Element Manager that you select.
6. Enter the relevant information and click **Save**.
7. Click **Commit**.

Adding a CallPilot profile for a user

Before you begin

A user must exist. To create a user, navigate to **User Management** > **New**.

About this task

For a communication profile, you can provide a maximum of one CallPilot mailbox. To add additional mailboxes for a user, you must add another communication profile.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a profile for a new user, click **New**.
   - To create a profile for an existing user, select the user and click **Edit**.
4. On the New User Profile page, click the **Communication Profile** tab.
5. In the CallPilot Messaging Profile section, select the check box and complete the following fields:
   - In the **System** field, select a CallPilot system. The system displays a list of systems that are registered with the element registry.
   - In the **Target** field, select the location of CallPilot, if provisioned.
   - In the **Template** field, select a template that CallPilot Element Manager provisions.
   - In the **Mailbox Number** field, enter a mailbox number for CallPilot.

     Note:

     You must enter the mailbox number even if the value is same as Primary DN.
6. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Adding a CS 1000 profile for a user

Before you begin

A user must exist . To create a new user, navigate to **User Management** > **New**.

About this task

For a communication profile, you can provide a maximum of one CS 1000 phone. To add additional phones for a user, you must add another communication profile.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, perform one of the following steps:
   - To create a profile for a new user profile, click **New**.
   - To create a profile for an existing user, select the user and click **Edit**.
4. On the New User Profile page, click the **Communication Profile** tab.
5. In the CS1000 Endpoint Profile section, select the check box and complete the following fields:
   - In the **System** field, select a CS 1000 system. The system displays a list of systems that are registered with the element registry.
   - In the **Target** field, select a CS 1000 customer number.
   - In the **Template** field, select a template that CS 1000 Element Manager provides.
   - In the **Primary DN** field, enter a preferred primary DN.

     Note:

     If you do not provide a primary DN, CS 1000 Element Manager automatically assigns a primary DN.
   - To exclude the profile in the CS 1000 corporate directory, clear the **Include in Corporate Directory** check box.
6. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Modifying a CS 1000 or CallPilot user profile

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the CS 1000 Endpoint Profile or CallPilot Messaging Profile section, enter the relevant information in the fields.

6. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Changing passwords of CS 1000 Presence users

Procedure

1. To log on to the System Manager personal agent console, enter `http://<SMGR server-name>/pa`.
2. Click **Change Password**.
3. Enter the old and new passwords, and then click **Save**.
   Presence Services recognizes the password change.

Note:

The system needs a synchronized password that is the same password as the password that Presence Services uses to update CS 1000.

B5800 Branch Gateway Profile Administration

Adding a B5800 Branch Gateway endpoint profile on a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a profile for a new user, click **New**.
   - To create a profile for an existing user, select the user and click **Edit**.
4. On the New User Profile page, click the **Communication Profile** tab.
5. Select the **B5800 Branch Gateway Endpoint Profile** checkbox.
6. Complete the **B5800 Branch Gateway Endpoint Profile** section.
7. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.

- To cancel the action and return to the previous page, click **Cancel**.

Related topics:

New User Profile field descriptions on page 361

Viewing a B5800 Branch Gateway endpoint profile of a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page select the user whose profile you want to view.
4. Click **View**.
5. Click the **Communication Profile** tab.

   Click the **B5800 Branch Gateway Endpoint** section to view the B5800 branch gateway endpoint profile of the user you selected.

Related topics:

New User Profile field descriptions on page 361

Modifying a B5800 Branch Gateway endpoint profile of a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the user whose profile you want to edit.
4. Click **Edit**.
5. Select the **Communication Profile** tab.
6. Edit the required fields in the **B5800 Branch Gateway Endpoint Profile** section.
7. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Related topics:

New User Profile field descriptions on page 361

Removing the association between a B5800 Branch Gateway endpoint profile and a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following:.
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. Clear the **B5800 Branch Gateway Endpoint Profile** checkbox.
6. Click **Commit**.

Managing default contact list of the user

Adding a contact in the Default Contact List

You can use this feature to add a contact to the contact list of the user.

Note:

To add a private contact, you must first create the private contact for the user. For more information, see Adding a private contact to a user on page 318.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following:
   - To add a contact for a new user, click **New**.
   - To add a new contact for an existing user, select a user and click **Edit**.
4. Click the **Contacts** tab.
5. In the Default Contact List section, enter a brief description of the contact list in the **Description** field.
6. In the Associated Contacts section, click **Add**.
7. On the Attach Contacts page, select one or more contacts and click **Select**.

The system displays the new contacts in the table in the Associated Contacts section.

Related topics:

Attach Contacts field descriptions on page 312

Modifying membership details of a contact in a contact list

About this task

You can use this feature to set speed dial and presence buddy information for the contacts in the Default Contact List.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Associated Contacts section, select a contact and click **Edit**.
6. On the Edit Contact List Member page, in the Contact Membership Details section, modify the required information in the fields.

   You can only modify the information in the fields displayed in the Contact Membership Details section. The fields marked with an asterisk (*) are mandatory fields.
7. Click **Add** .
8. Click **Commit** to save the changes.

Related topics:

Edit Contact List Member field descriptions on page 314

Viewing membership details of a contact in the contact list

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.

4. On the User Profile View page, click the **Contacts** tab.
5. In the Associated Contacts section, click the last name link under the **Last Name** column.

Result

The View Contact List Member page displays the details of the selected contact.

Related topics:

View Contact List Member field descriptions on page 316

Deleting contacts from the default contact list

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. Select one or more contacts from the Associated Contacts section and click **Remove**.

Attach Contacts field descriptions

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Scope	Displays the categorization of the contact based on whether the contact is a user, public, or private contact.
Display/Login Name	Displays the unique login name or display name of the contact.
Contact Address	Displays the address of a private or public contact. No contact address is associated with a contact type user.
User Handles	Displays the communication handles associated with the user. These handles are

Name	Description
	defined in the communication profile of a user.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays fields under selected columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.
Advanced Search	Displays fields that you can use to specify the search criteria to search for contacts.

Button	Description
Select	Adds the selected contact in the list of associated contacts.
Cancel	Cancels your selection and takes you to the Contacts tab.

The page displays the following field when you click the **Advanced Search** button at the upper-right corner of the contact table.

Name	Description
Search On	Specifies whether the search must base on the **Contact** or **User**.
Criteria	Defines the search criteria for searching the contacts. Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search the contacts. You can search based on the first name, last name, or the address/handle of the contact. • Drop-down 2 - The operators for evaluating the expression. Based on the search criterion which you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down field. • Field 3 - The value for the search criterion.

Button	Description
+	Adds one more search criteria section.

Button	Description
-	Clears the last search criteria. This button is applicable only if there is more than one search criteria.

Edit Contact List Member field descriptions

Contact Membership Details

Name	Description
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This field is similar to **Label**, but it is used to store label in an alternate language.
Description	Displays a brief description about the contact.
Presence Buddy	Provides the option to indicate whether to allow monitoring of the presence information of the contact.
Speed Dial	Provides the option to indicate whether to allow speed dial for the contact.
Address/Handle	Displays a fully qualified URI for interacting with the contact. This field is available only if you select the **Speed Dial** check box.
Speed Dial Entry	Displays the reduced number that represents the speed dial number. This field is available only if you select the **Speed Dial** check box.

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description about the contact.
Company	Displays the name of contact's company

Name	Description
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set a language as the preferred language for the contact.
Update Time	Displays the time when the contact information was last updated.
Source	Displays the source of provisioning the contact.

Postal Address

Name	Description
Name	Displays the name of the contact.
Address Type	Displays the type of mailing address such as, home or office address.
Street	Displays the name of the street.
Locality Name	Displays the name of the city or town.
Postal Code	Displays the postal code of the locality of the city or town.
Province	Displays the full name of the contact's province.
Country	Displays the name of the contact's country.

Contact Address

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.
Type	Displays the type of communication medium for interacting with the user.
Category	Displays the categorization of the address based on the location.
Label	Displays the text description for classifying this contact.

Name	Description
Alternative Label	Displays the text description for classifying this contact. This field is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Add	Saves the modified information in the database.

View Contact List Member field descriptions

Contact Membership Details

Name	Description
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. The **Alternative Label** field is similar to **Label**, but you use the field to store label in an alternate language.
Description	Displays a brief description about the contact.
Presence Buddy	Provides the option to indicate whether to allow monitoring of the presence information of the contact.
Speed Dial	Provides the option to indicate whether to allow speed dial for the contact.
Address/Handle	Displays a fully qualified URI for interacting with the contact. This field is available only if you select the **Speed Dial** check box.
Speed Dial Entry	Displays the reduced number that represents the speed dial number. This field is available only if you select the **Speed Dial** check box.

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.

Name	Description
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description about the contact.
Company	Displays the name of contact's company
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.
Update Time	Displays the time when the contact information was last updated.
Source	Displays the source of provisioning the contact.

Postal Address

Name	Description
Name	Displays the name of the contact.
Address Type	Displays the mailing address type such as, home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code of the locality of the city or town.
Province	Displays the full name of the contact's province.
Country	Displays the name of the contact's country.

Contact Address

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.
Type	Displays the type of communication medium for interacting with the user.

Name	Description
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This field is similar to **Label**, but it is used to store label in an alternate language.

Managing private contacts of a user

Adding a private contact to a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To add a private contact while setting up a new user, click **New**.
   - To add a private contact to an existing user, select the user and click **Edit**.
4. Click the **Contacts** tab.
5. In the Private Contacts section, click **New**.
6. On the New Private Contact page, enter the last name, first name, middle name, description, company name, localized display name, endpoint display name, and language preference in the Contact Details section.

   The fields marked with the asterisk (*) are mandatory. You must enter a valid information in these fields.
7. In the Postal Address section, click **New** to choose a postal address for the contact.

   You can click **Choose Shared Address** to choose a shared address for a contact.
8. In the Contact Address section, click **New** to choose a contact address for the contact.
9. Click **Add** to add the private contact.
10. Click **Commit** to save the contact as the private contact of the user.

Note:

Before you click **Commit**, ensure that all the mandatory fields marked with asterisk (*) have valid information.

Related topics:

New Private Contact field descriptions on page 325

Modifying details of a private contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select a contact.
6. Click **Edit**.
7. On the Edit Private Contact page, modify the contact's information.
8. Click **Add** to save the modified information.

Related topics:

Edit Private Contact field descriptions on page 327

Viewing details of a private contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. On the User Profile View page, click the **Contacts** tab.
5. Click **Private Contacts**.
6. In the Private Contacts section, click the link displayed in the **Last Name** column for a contact.

The View Private Contact page displays the details of the contact whose last name you have clicked.

Related topics:

View Private Contact field descriptions on page 329

Deleting private contacts of a user

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select one or more contacts from the table displaying private contacts.
6. Click **Delete**.
7. On the **Contact Delete Confirmation** page, click **Delete**.
8. On the User Profile Edit page, click **Commit**.

Adding a postal address of a private contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - If you are adding a postal address of a private contact to a new user, click **New**.
   - If you are adding a postal address of a private contact to an existing user, select a user and click **Edit**.
4. Click the **Contacts** tab.
5. In Private Contacts section, perform one of the following steps:
   - If you are adding a postal address for a new private contact, click **New**.

- If you are adding a postal address for an existing private contact, select a private contact and click **Edit**.

6. On the New Private Contact or Edit Private Contact page, click **New** in the Postal Address section.
7. On the Add Address page, enter the required information in the respective fields.

   The fields marked with asterisk (*) are mandatory. You must enter valid information in these fields.
8. Click **Add** to create a new postal address for the private contact.

Related topics:

Add Address field descriptions on page 99

Modifying postal address of a private contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select an address from the Postal Address section.
7. Click **Edit**.
8. On the Edit Address page, modify the information in the respective fields.

   The fields marked with asterisk (*) are mandatory. You must enter valid information in these fields.
9. Click **Add**.
10. Click **Commit** to save the modified address.

Related topics:

Edit Address field descriptions on page 101

Deleting postal addresses of a private contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select one or more addresses from the Postal Address section.
7. Click **Delete**.
8. Click **Commit**.

Choosing a shared address for a private contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To choose a shared address for a private contact while creating a new user, click **New**.
   - To choose a shared address for a private contact of an existing user, select the user and click **Edit**.
4. Click the **Contacts** tab.
5. In the Private Contacts section, perform one of the following actions:
   - To add a new contact and add a address to it, click **New**.
   - To add an address to an existing contact, select the contact and click **Edit**.
6. On the New Private Contact or the Edit Private Contact page, click **Choose Shared Address** in the Postal Address section.
7. On the Choose Address page, select one or more shared addresses.
8. Click **Select**.
9. Click **Add** to add the selected addresses to the private contact.

10. Click **Commit** to save the private contact information.

Related topics:

Choose Address field descriptions on page 102

Adding a contact address of a private contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To add a contact address of a private contact while setting up a new user, click **New**.
   - To add a contact address of a private contact for an existing user, select the user and click **Edit**.
4. Click the **Contacts** tab.
5. In the Private Contacts section, perform one of the following steps:
   - To add a contact address for a new private contact, click **New**.
   - To add a contact address for an existing private contact, select the private contact from the table and click **Edit**.
6. On the New Private Contact or the Edit Private Contact page, click **New** in the Contact Address section.
7. On the Add Address page, enter the appropriate information in the respective fields.

   The fields marked with asterisk (*) are mandatory. You must enter a valid information in these fields.
8. Click **Add**.
9. Click **Commit**.

Related topics:

Add Address field descriptions on page 331

Modifying a contact address of a private contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select a contact address from the Contact Address section.
7. Click **Edit**.
8. On the Edit Address page, modify the information in the respective fields.

   The fields marked with asterisk (*) are mandatory. You must enter valid information in these fields.
9. Click **Add** to save the modified address.
10. On the Edit Private Contact page, click **Add**.
11. On the User Profile Edit page, click **Commit**.

Note:

Ensure that all the mandatory fields have valid information before you click **Commit**.

Related topics:

Edit Address field descriptions on page 332

Deleting contact addresses of a private contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contact section, select a contact and click **Edit**.

6. On the Edit Private Contact page, select one or more addresses from the Contact Address section.
7. Click **Delete**.
8. Click **Commit**.

New Private Contact field descriptions

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description about the contact.
Company	Displays the name of contact's company.
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.

Postal Address

Name	Description
Name	Displays the unique label that identifies the address.
Address Type	Displays the mailing address type such as, home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town of the contact.
Postal Code	Displays the postal code of the of the city or town where the contact's office or home is located.

Name	Description
Province	Displays the full name of the province where the contact's office or home is located.
Country	Displays the name of the country where the contact's office or home is located.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to modify an existing postal address of the private contact.
New	Opens the **Add Address** page. Use this page to add a new postal address of the private contact.
Delete	Deletes the selected postal address.
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the private contact.

Contact Address

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.
Type	Displays the type of communication medium for interacting with the user.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This field is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the private contact.

Button	Description
New	Opens the **Add Address** page. Use this page to add a contact address of the private contact.
Delete	Deletes the selected contact address.

Button	Description
Add	Creates a new contact. **Note:** You must enter valid information in the mandatory fields to successfully create a new contact.

Edit Private Contact field descriptions

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description about the contact.
Company	Displays the name of contact's company
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.
Update Time	Displays the time when the contact information was last updated.
Source	Displays the source of provisioning the contact.

Postal Address

Name	Description
Name	Displays the unique label that identifies the address.
Address Type	Displays the mailing address type such as, home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code of the of the city or town where the contact's office or home is located.
Province	Displays the full name of the province where the contact's office or home is located.
Country	Displays the name of the country where the contact's office or home is located.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to modify an existing postal address of the private contact.
New	Opens the **Add Address** page. Use this page to add new postal address of the private contact.
Delete	Deletes the selected contact address.
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the private contact.

Contact Address

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.
Type	Displays the type of communication medium for interacting with the user.
Category	Displays the categorization of the address based on the location.

Name	Description
Label	Displays the text description for classifying this contact.
Alternative Label	Displays the text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the private contact.
New	Opens the **Add Address** page. Use this page to add a contact address of the private contact.
Delete	Deletes the selected private contacts.

Button	Description
Add	Saves the modified information to the database.

View Private Contact field descriptions

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description about the contact.
Company	Displays the name of contact's company
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.

Name	Description
Update Time	Displays the time when the contact information was last updated.
Source	Displays the source of provisioning the contact.

Postal Address

Name	Description
Name	Displays the unique label that identifies the address.
Address Type	Displays the mailing address type such as, home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code of the of the city or town where the contact's office or home is located.
Province	Displays the full name of the contact's province.
Country	Displays the name of the contact's country.

Contact Address

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.
Type	Displays the type of communication medium used to interact with the user.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Done	Takes you to the previous page.

Add Address field descriptions

Use this page to add communication address of the contact.

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, SIP, or IM of the contact. The format of the address must conform to the type of address that you select in the **Type** field.
Type	Displays the type of address. The types of addresses are: • **Phone**: This address type supports phone numbers. • **SIP**: This address type supports SIP-based communication. • **MSRTC**: This address type supports communication with a Microsoft RTC server. • **IBM Sametime**: This address type supports communication with IBM Sametime. • **XMPP**: This address type supports xmpp-based communication. • **SMTP**: This address type supports communication with the SMTP server.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Add	Adds the contact address of the public contact to the database.

Related topics:

Adding a contact address of a public contact on page 402

Edit Address field descriptions

Use this page to edit the details of a contact's communication address.

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, SIP, or IM of the contact. The format of the address must conform to the type of address that you select in the **Type** field.
Type	Displays the type of address. The types of addresses are: • **Phone**: This address type supports phone numbers. • **SIP**: This address type supports SIP-based communication. • **MSRTC**: This address type supports communication with a Microsoft RTC server. • **IBM Sametime**: This address type supports communication with IBM Sametime. • **XMPP**: This address type supports xmpp-based communication. • **SMTP**: This address type supports communication with the SMTP server.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Add	Saves the modified information to the database.

Related topics:

Modifying the details of a public contact on page 403

User Management field descriptions

The User Management module is the primary master of the user profile. It provides Avaya customers and Avaya products with a single point of administration for creating, viewing, modifying, and deleting users. This page has two sections. The upper section contains buttons that you can use to:

- create, view, modify, and delete users
- assign roles to a user
- add a user to a group

The lower section contains a table that displays information about the user.

Name	Description
Last Name	Displays the last name of the user
First Name	Displays the first name of the user.
Display Name	Displays the unique name of the user displayed by the system.
Login Name	Displays the unique name that gives access to the system.
E164 Handle	Displays the unique communication address of the user.
Last Login	Displays the date and time when the user successfully logged into the system.

Button	Description
View	Opens User Profile View page that you can use to view the details of the selected user.
Edit	Opens the User Profile Edit page that you can use to modify the details of the selected user.
New	Opens the New User Profile page that you can use to create a new user.
Duplicate	Opens the User Profile Duplicate page that you can use create a duplicate user.

Button	Description
Delete	Opens the User Delete Confirmation page that you can use to temporarily delete the selected users.
More Actions > **Assign Roles**	Opens the Assign Roles page that you can use to assign roles to the selected users.
More Actions > **Add To Group**	Opens the Assign Groups page that you can use to assign groups to the selected users .
More Actions > **Show Deleted User**	Opens the Deleted Users page that you can use to view, permanently delete, and restore the deleted users .
Advanced Search	Displays fields that you can use to specify the search criteria for searching a user.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters users based on the filter criteria.
Select: All	Selects all the users in the table.
Select: None	Clears the check box selections.
Refresh	Refreshes the user information in the table.

Criteria

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Criteria	Displays the following three fields: • Field 1 – Lists the criteria that you can use to search users. • Field 2 – Lists the operators for evaluating the expression. The operators displayed depends on the criterion you selected in the first field. • Field 3 – Lists the value for the search criterion. The User Management service retrieves and displays users that match this value.

User Profile View field descriptions

Use this page to view the details of the selected user account.

The User Profile View page has the following four tabs:

- **Identity**
- **Communication Profile**
- **Membership**
- **Contacts**

Identity tab — Identity section

Name	Description
Last Name	The last name of the user. The selection is required.
First Name	The first name of the user. The selection is required.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Status	Displays the login status of the user.
Update Time	Displays the time when the user details were last modified.
Login Name	The unique system log-in name given to the user. The log-in name takes the form of username@domain. You use the log-in name to create the user's primary handle. The log-in name is caseinsensitive. For example, if you enter TEST@AVAYA.COM, the system converts the log-in name to lowercase, that is, test@avaya.com. However, on the log-in page, you can enter TEST@AVAYA.COM or test@avaya.com. The log-in name can be in uppercase or lowercase. You cannot edit the **Login Name** field for users with the log-in name admin.
Authentication Type	Authentication type defines how the system performs user authentication. The options are:

Name	Description
	• **Enterprise**: User login is authenticated by the enterprise. • **Basic**: User login is authenticated by an Avaya Authentication Service.
Source	Specifies the entity that created this user record. The possible values for this field is either an IP Address/Port, or a name representing an enterprise LDAP, or Avaya.
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.
Title	Displays the personal title for address a user. This is typically a social title and not the work title.
Language Preference	Displays the preferred written or spoken language of the user.
Time Zone	Displays the preferred time zone of the user.
Employee ID	The employee number for the user.
Department	The department which the user belongs to.
Company	The organization where the user works.

Identity tab — Address section

Name	Description
Name	Displays the unique label that identifies the address.
Address Type	Displays the type of the address. Types of addresses are: • Office • Home
Street	Displays the name of the street.
City	Displays the name of the city or town.

Name	Description
Postal Code	Displays the postal code used by postal services to route mail to a destination. In United States, this is Zip code.
Province	Displays the full name of the province.
Country	Displays the name of the country.

Identity tab — Localized Names section

Name	Description
Language	Specifies the localized languages for displaying the user name.
Display Name	Displays the user name in the localized language you choose.

Button	Description
New	Allows you to add a new localized name for the user.
Edit	Allows you to edit the localized name for the user.
Delete	Deletes the localized names you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	Cancels your add or edit of the localized name.

Communication Profile tab — Communication Profile section

Name	Description
Option	Displays the details of the selected communication profile.
Name	Displays the name of the communication profile.

Name	Description
Name	Displays the name of the communication profile for the user.
Default	Displays the profile that is made default as the active profile. There can be only one active profile at a time.

Communication Profile tab — Communication Address section

Name	Description
Type	Displays the type of the handle.
Handle	Displays the unique communication address for the user.
Domain	Displays the name of the domain with which the handle is registered.

Communication Profile tab — Session Manager section

Note:

The system displays the following fields only if a communication profile of the user exists for the product.

Name	Description
Primary Session Manager	Select the Session Manager instance that you use as home server for the currently displayed Communication Profile. As a home server, the selected primary Session Managerinstance will be used as the default access point for connecting devices associated with the Communication Profile to the Avaya network. A selection is required.
Secondary Session Manager	If you select a secondary Session Manager instance, this Session Manager provides continued service to SIP devices associated with this Communication Profile when the primary Session Manager becomes unavailable. A selection is optional.
Origination Application Sequence	Select an Application Sequence that will be invoked when the system routes the calls from this user. A selection is optional. **Note:** If an origination and a termination application sequences are specified, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional.

Name	Description
	Note: If an origination and a termination application sequences are specified, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Conference Factory Set	The Conference Factory Set contains a set of Well Known Conference URIs that you can use as conference server to initiate conference calls. If the system has Conference Factory Set administered, you can get the list of Well Known Conference URIs. You require the URIs to initiate conference calls.
Survivability Server	For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to the Communication Manager survivable remote server resident with the Branch Session Manager. A selection is optional. **Note:** If a termination or origination application sequence contains a Communication Manager application, the Communication Manager associated with the application must be the main Communication Manager for the Communication Manager survivable remote server that is resident with the Branch Session Manager.
Home Location	This field is specified to support mobility for the currently displayed user. This is used by Session Manager when the IP address of the calling phone does not match any IP address pattern of any location.

Communication Profile tab — CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Name/Button	Description
System	Displays the Communication Manager on which you add the endpoint. The Communication Manager system on which you add the endpoint. The selection is required.
Profile Type	Displays the type of the profile for the user.
Extension	The extension of the endpoint that you associate this profile with. The selection is required.
View Endpoint	Lists the existing or available endpoints based on check box status of the **Use Existing Endpoints** field.
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. The selection is required.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Provides numeric only handles, SIP or nonSIP, that are administered for a user. The **Preferred Handle** field is optional. By default the field is not set to any value. If SIP entity is of Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Delete Endpoint on Unassign of Endpoint from User or Delete User	Use this check box to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.
Override Endpoint Name	Use this check box for the following two purposes: • To override the endpoint name on Communication Manager with the value

Name/Button	Description
	you configured on the Manage Users page during synchronization. If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization. • To override the Localized Display Name on the Manager Users page on the **Native Name** field of Communication Manager. If you clear the check box, the system does not override the Localized display name in the **Native Name** field.

Communication Profile tab - CS1000 Endpoint Profile

Field	Description
System	The CS1000 system of the station you view.
Target	The system customer number for the Communication Server.
Template	The phone or endpoint template that you can choose for the user. Select a template from the drop down list. The element manager maintains all the templates.
Update	Updates the station profile information for the user. When you click this button, the system takes you to the element manager cut through for the updates.
Service Details	Displays service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field.
Include in Corporate Directory	Select this check box to add this profile to the CS1K Corporate Directory feature.

Communication Profile tab — Messaging Profile

Note:

The system displays the following fields only if a messaging profile can be configured for the user.

Name	Description
System	Displays the Messaging System on which you add the subscriber.
Template	Displays the template, system-defined or user-defined, that you associate with the subscriber.
Mailbox Number	Displays the mailbox number of the subscriber.
Password	The password for logging on to the mailbox.
Delete Subscriber on Unassign of Subscriber from User	Provides the option to specify whether to delete the subscriber mailbox from the Messaging device or Communication System Management when you remove this messaging profile or when you delete the user.

Communication Profile tab - CallPilot Messaging Profile

Field	Description
System	The CallPilot system of the mailbox to view.
Location	This field maps to the CallPilot Location field. CallPilot Manager provides the **Location** field.
Template	The mailbox template you apply. Select a template from the drop down list. The element manager maintains all the mailbox templates.
Update	Updates the mailbox information for the user. If you click **Update**, the system cuts through to the element manager for the updates.
Service Details	Displays mailbox service details from endpoint after you create the mailbox.
Mailbox Number	Mailbox number or the extension DN of the user.

Communication Profile tab — B5800 Branch Gateway Endpoint Profile

Use this profile to assign a new or an existing user to a B5800 Branch Gateway device in user management.

While adding a user, if you have opted to assign a CM Endpoint Profile and a B5800 Branch Gateway Endpoint Profile to the user, then the B5800 Branch Gateway Endpoint Profile is used as survivability option for the CM Endpoint Profile. That is, the endpoint extension used in the CM Endpoint Profile is also used for creating a B5800 Branch Gateway Endpoint Profile so

that when Communication Manager is unavailable, the B5800 Branch Gateway device can serve the extension.

Note:

If a CM Endpoint Profile is present while adding or editing a user, the user administration is considered to be in Centralized Mode, else the user administration is be considered to be in Distributed Mode.

Before you configure the B5800 Branch Gateway Endpoint Profile details, if the system has to populate the CM Endpoint Profile data or CS1000 Endpoint Profile data in the B5800 Branch Gateway Endpoint Profile fields, you must click **Commit & Continue**.

You can have a B5800 Branch Gateway Endpoint Profile as a survivable option to a CS1000 Station profile.

Name/Button	Description
System	Displays a list of B5800 Branch Gateway device names from which you can select the B5800 Branch Gateway device you associate with the user.
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint you associate. The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Set Type	Displays the set type for the B5800 endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the set type gets auto populated.
Template	Displays a list of user templates from which you can select your preferred template to set the user configurations.
Endpoint Editor button	Starts the Avaya Aura® B5800 Branch Gateway Manager application where, you can edit or view details of the B5800 endpoint. After you save the changes in Avaya Aura® B5800 Branch Gateway Manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Delete Extension On User Delete check box	Provides the option to delete the extension associated with the user while deleting the

Name/Button	Description
	user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Membership tab — Roles section

Name	Description
Name	Displays the name of the role.
Description	Displays a brief description about the role.

Membership tab — Group Membership section

Name	Description
Name	Displays the name of the group.
Type	Displays the group type based on the resources.
Hierarchy	Displays the position of the group in the hierarchy.
Description	Displays a brief description about the group.

Contacts tab — Default Contact List section

Name	Description
Description	Displays a brief description of the contact list.

Contacts tab — Associated Contacts section

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Scope	Displays the categorization of the contact based on whether the contact is a public or private contact.
Speed Dial	Displays the value that specifies whether the speed dial is set for the contact.
Speed Dial Entry	Displays the reduced number that represents the speed dial number.

Name	Description
Presence Buddy	Displays the value that specifies whether you can monitor the presence information of the contact or not. **False** indicates that you cannot track the presence of the contact.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab — Private Contacts section

Use this section to add new private contacts, modify and deletes existing contacts.

Name	Description
Last Name	Displays the last name of the private contact.
First Name	Displays the first name of the private contact.
Display Name	Display name of the private contact.
Contact Address	Displays the address of the private contact.
Description	Displays a brief description about the contact.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Edit	Opens the User Profile Edit page. Use the User Profile Edit page to modify the details of the user account.
Done	Closes the User Profile View page and takes you back to the User Management page.

User Profile Edit field descriptions

Use this page to modify the details of a user account.

The User Profile Edit page has the following four tabs:

- **Identity**
- **Communication Profile**
- **Membership**
- **Contacts**

Identity tab — Identity section

Name	Description
Last Name	The last name of the user. The selection is required.
First Name	The first name of the user. The selection is required.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Status	The login status of the user
Update Time	The time when the user details were last modified.
Login Name	The log-in name of the user. The selection is required. The log-in name is caseinsensitive. For example, if you enter TEST@AVAYA.COM, the system converts the log-in name to lowercase, that is, test@avaya.com. However, on the log-in page, you can enter TEST@AVAYA.COM or test@avaya.com.

Name	Description
	The log-in name can be in uppercase or lowercase. If you log in to the system as admin, you cannot edit the **Login Name** field.
Authentication Type	The type of authentication that defines how the system performs the authentication of user. The selection is required. The options are: • **Enterprise**: Login of the user is authenticated by the directory servers that are external to System Manager. • **Basic**: Login of the user is authenticated by an Avaya Authentication Service.
Change Password	Enter a new password. The selection is required.
Source	Specifies the entity that created this user record. The possible values for this field is either an IP Address/Port, or a name representing an enterprise LDAP, or Avaya.
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.
Title	The personal title that is set to address a user. This is typically a social title and not the work title.
Language Preference	The preferred written or spoken language of the user.
Time Zone	The preferred time zone of the user.
Employee ID	The employee number for the user.
Department	The department which the user belongs to.
Company	The organization where the user works.

Identity tab — Address section

Name	Description
Time Zone	The preferred time zone of the user.
Department	The department which the user belongs to.

Name	Description
Address Type	The type of address. The values are: • **Office** • **Home**
Street	The name of the street.
City	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. For United States, the postal code is the Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
New	Opens the Add Address page. Use the page to add the address details.
Edit	Allows you to modify the address.
Delete	Deletes the selected address.
Choose Shared Address	Opens the Choose Address page that you can use to choose a shared or common address.

Identity tab — Localized Names section

Name	Description
Language	The localized languages for displaying the user name. The selection is required.
Display Name	The user name in the localized language you choose. The selection is required.

Button	Description
New	Allows you to add a new localized name for the user.
Edit	Allows you to edit the localized name for the user.
Delete	Deletes the localized names you select for the user.
Add	Adds or edits the localized name for the user.

Button	Description
Cancel	Cancels your add or edit of the localized name.

Communication Profile tab — Communication Profile section

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Communication Profile Password	Type your communication profile password.
Option button	Use this button to view the details of the selected communication profile.
Name	Name of the communication profile. The selection is required.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding a communication profile.

The system enables the following fields when you click the **New** button in the Communication Profile section.

Name	Description
Name	The name of the communication profile for the user.
Default	The profile that is made default as the active profile. There can be only one active profile at a time.

Communication Profile tab — Communication Address section

Use this section to create, modify, and delete the communication address of a user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Type	The type of the handle.
Handle	A unique communication address of the user.

Name	Description
Domain	The name of the domain with which the handle is registered.

Button	Description
New	The fields for adding a new communication address.
Edit	Use this button to edit the information of a selected communication address.
Delete	Deletes the selected communication address.

The page displays the following fields when you click **New** or **Edit** in the Communication Address section.

Name	Description
Type	The type of the handle. The different types of handles are: • **Avaya SIP**: Indicates that the handle supports Avaya SIP-based communication. • **Avaya E.164**: Indicates that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. • **Microsoft OCS SIP**: Indicates that the handle supports OCS SIP-based communication. • **Microsoft Exchange**: Signifies that the handle is an e-mail address and supports communication with Microsoft SMTP server. • **Lotus Notes**: Indicates that the handle is for Lotus Notes and domino calender. • **IBM Sametime**: Indicates that the handle is for IBM Sametime. • **Avaya XMPP**: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP)-based communication with the Jabber service. • **GoogleTalk**: Indicates that the handle supports XMPP-based communication with the Google Talk service.

Name	Description
	• **Other Email**: Indicates that the handle is an e-mail address other than MS Exchange e-mail addresses. • **Other SIP**: Indicates that the handle supports other SIP-based communication than the ones mentioned above. • **Other XMPP**: Indicates that the handle supports other XMPP-based communication than the ones mentioned above.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user, or an address of an communication device using which user can send or receive messages. The selection is required.

Button	Description
Add	Saves the new communication address or modified communication address information in the database.
Cancel	Cancels the addition of communication address.

Communication Profile tab — Session Manager

Note:

The system displays the following fields only if a communication profile of the user exists for the product.

Name	Description
Primary Session Manager	Select the Session Manager instance that must be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.
Secondary Session Manager	If a secondary Session Manager instance is selected, this Session Manager provides continued service to SIP devices associated with this Communication Profile when the

Name	Description
	primary Session Manager becomes unavailable. A selection is optional.
Origination Application Sequence	Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. **Note:** If an origination and a termination application sequences are specified, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional. **Note:** If an origination and a termination application sequences are specified, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Conference Factory Set	The Conference Factory Set contains a set of Well Known Conference URIs that you can use as conference server to initiate conference calls. If the system has Conference Factory Set administered, you can get the list of Well Known Conference URIs. You require the URIs to initiate conference calls.
Survivability Server	For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a Communication Profile when the local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional.

Name	Description
	Note: If a termination or origination application sequence contains a Communication Manager application, Communication Manager associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.
Home Location	Specify a Home Location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any of the location. The selection is required.

Communication Profile tab — CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Name/Button	Description
System	The Communication Manager system on which you add the endpoint. The selection is required.
Profile Type	The type of the Communication Manager Endpoint profile you require to create. The selection is required.
Use Existing Endpoints	Select the check box to use the existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint that you associate this profile with. The selection is required. The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Template	The template, system defined or user defined, you associate with the endpoint. Select the template based on the set type you add. The selection is required.

Name/Button	Description
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. The selection is required. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Provides numeric only handles, SIP or nonSIP, that are administered for a user. The **Preferred Handle** field is optional. By default the field is not set to any value. If the SIP entity is of the Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Delete Endpoint on Unassign of Endpoint from User or on Delete User	Use this check box to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.
Override Endpoint Name	Use this check box to override the following endpoint names: • The endpoint name on Communication Manager with the value you configured on the Manage Users page during synchronization. If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization. • The Localized Display Name on the Manager Users page on the **Native Name** field of Communication Manager. If you clear the check box, the system does not override the Localized display name in the **Native Name** field.

Communication Profile tab - CS1000 Endpoint Profile

Field	Description
System	The CS 1000 system on which you add a phone. The selection is required.
Target	The system customer number for the Communication Server. The selection is required.
Template	The phone or endpoint template that you can choose for the user. Select a template from the drop down list. The element manager maintains all the templates. The selection is required.
Update	Updates the station profile information for the user. When you click **Update**, the system takes you to the element manager cut through for the updates.
Service Details	Displays service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field.
Include in Corporate Directory	Use to add this profile to the CS1K Corporate Directory feature.

Communication Profile tab — Messaging Profile section

Note:

The system displays the following fields only if a messaging profile can be configured for the user.

Name	Description
System	The messaging system on which you add the subscriber. The selection is required.
Use Existing Subscriber on System	Use to specify whether to use an existing subscriber mailbox number to associate with this profile.
Mailbox Number	The mailbox number of the subscriber. The selection is required. The field takes the existing mailbox number that you associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.

Name	Description
Messaging Editor button	Click to start the messaging application where, you can edit or view details of the profile of the messaging endpoint. After you save the changes in messaging, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Template	The system-defined or user-defined template you associate with the subscriber.
Password	The password for logging in to the mailbox. The selection is required.
Preferred Handle	Provides numeric only handles, SIP or nonSIP, that are administered for a user. The **Preferred Handle** field is optional. By default the field is not set to any value. If the SIP entity is of the Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	Use to specify whether to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user.

Communication Profile tab - CallPilot Messaging Profile

Field	Description
System	The CallPilot system of the messaging profile you edit. The selection is required.
Target	This field maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. The selection is required.
Template	The mailbox template you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. The selection is required.
Update	Updates the mailbox information for the user. If you click the **Update** button, the system cuts through to the element manager for the updates.

Field	Description
Service Details	Displays mailbox service details from endpoint after you create the mailbox.
Mailbox Number	The mailbox number or the extension DN of the user. The selection is required.

Communication Profile tab — B5800 Branch Gateway Endpoint Profile

Use this profile to assign a new or an existing user to a B5800 Branch Gateway device in user management.

While adding a user, if you have opted to assign a CM Endpoint Profile and a B5800 Branch Gateway Endpoint Profile to the user, then the B5800 Branch Gateway Endpoint Profile is used as survivability option for the CM Endpoint Profile. That is, the endpoint extension used in the CM Endpoint Profile is also used for creating a B5800 Branch Gateway Endpoint Profile so that when Communication Manager is unavailable, the B5800 Branch Gateway device can serve the extension.

Note:

If a CM Endpoint Profile is present while adding or editing a user, the user administration is considered to be in Centralized Mode, else the user administration is be considered to be in Distributed Mode.

Before you configure the B5800 Branch Gateway Endpoint Profile details, if the system has to populate the CM Endpoint Profile data or CS1000 Endpoint Profile data in the B5800 Branch Gateway Endpoint Profile fields, you must click **Commit & Continue**.

You can have a B5800 Branch Gateway Endpoint Profile as a survivable option to a CS1000 Station profile.

Name/Button	Description
System	Displays a list of B5800 Branch Gateway device names from which you can select the B5800 Branch Gateway device you associate with the user. The selection is required.
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint you associate with. The selection is required. The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Set Type	Displays the set type for the B5800 endpoint profile. By default the **Set Type** field is

Name/Button	Description
	disabled. If you select a template, the set type gets auto populated.
Template	Displays a list of user templates from which you can select your preferred template to set the user configurations. The selection is required.
Endpoint Editor button	Starts the Avaya Aura® B5800 Branch Gateway Manager application where, you can edit or view details of the B5800 endpoint. After you save the changes in Avaya Aura® B5800 Branch Gateway Manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Delete Extension On User Delete check box	Provides the option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Membership tab — Roles section

Name	Description
check box	Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account.
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Assign Roles	Opens the Assign Role page that you can use to assign the roles to the user account.
Unassign Roles	Removes the selected role from the list of roles associated with the user account.

Membership tab — Group Membership section

Name	Description
check box	Use this check box to select a group.

Name	Description
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Button	Description
Add To group	Opens the Assign Groups page that you can use to add the user to a group.
Remove From Group	Removes the user from the selected group.

Contacts tab — Default Contact List

Name	Description
Description	A brief description of the contact list.

Contacts tab — Associated Contacts

Name	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Scope	Categorization of the contact based on whether the contact is a public or private contact.
Speed Dial	The value specifies whether the speed dial is set for the contact or not.
Speed Dial Entry	The reduced number that represents the speed dial number.
Presence Buddy	The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact.

Button	Description
Edit	Opens the Edit Contact List Member page. Use this page to modify the information of the selected contact.
Add	Opens the Attach Contacts page. Use this page to select one or more contacts from the list of contacts.

Button	Description
Remove	Removes one or more selected contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab — Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

Name	Description
Last Name	Last name of the private contact.
First Name	The first name of the contact.
Display Name	Display name of the private contact.
Contact Address	Address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Opens the Edit Private Contact page. Use this page to modify the information of the contact you selected.
New	Opens the **New Private Contact** page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Commit & Continue	Saves your changes and retains you on the same page for further modifications.
Commit	Modifies the user account and takes you back to the User Management or User Profile View page. **Note:** While restoring a deleted user, use the **Commit** button to restore a deleted user.
Cancel	Cancels the operation of modifying the user information and takes you back to the User Management or User Profile View page.

New User Profile field descriptions

Use this page to create a new user. This page has four tabs:

- **Identity**
- **Communication Profile**
- **Membership**
- **Contacts**

Note:

The fields that are marked with an asterisk are mandatory and you must enter appropriate information in these fields.

Identity tab — Identity section

Name	Description
Last Name	The last name of the user. The selection is required.
First Name	The first name of the user. The selection is required.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Login Name	The log-in name of the user. The selection is required.

Name	Description
	The log-in name is caseinsensitive. For example, if you enter TEST@AVAYA.COM, the system converts the log-in name to lowercase, that is, test@avaya.com. However, on the log-in page, you can enter TEST@AVAYA.COM or test@avaya.com. The log-in name can be in uppercase or lowercase. If you log in to the system as admin, you cannot edit the **Login Name** field.
Authentication Type	The type of authentication that defines how the system performs the authentication of user. The selection is required. The options are: • **Enterprise**: Login of the user is authenticated by the directory servers that are external to System Manager. • **Basic**: Login of the user is authenticated by an Avaya Authentication Service.
Password	The password you choose. The selection is required.
Confirm Password	The password that you re-enter for confirmation. The selection is required.
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.
Title	The personal title that is set to address a user. This is typically a social title and not the work title.
Language Preference	The preferred written or spoken language of the user.
Time Zone	The preferred time zone of the user.
Employee ID	The employee number for the user.
Department	The department which the user belongs to.
Company	The organization where the user works.

Identity tab — Address section

Name	Description
Select check box	Use this check box to select an address in the table.
Name	The name of the addressee.
Address Type	The type of address. The values are: • **Office** • **Home**
Street	The name of the street.
City	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. For United States, the postal code is the Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
New	Opens the Add Address page. Use the page to add the address details.
Edit	Allows you to modify the address.
Delete	Deletes the selected address.
Choose Shared Address	Opens the Choose Address page that you can use to choose a shared or common address.

Identity tab — Localized Names section

Name	Description
Language	The localized languages for displaying the user name. The selection is required.
Display Name	The user name in the localized language you choose. The selection is required.

Button	Description
New	Allows you to add a new localized name for the user.
Edit	Allows you to edit the localized name for the user.

Button	Description
Delete	Deletes the localized names you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	Cancels your add or edit of the localized name.

Communication Profile tab — Communication Profile section

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Communication Profile Password	Type your communication profile password.
Confirm Password	Enter your communication profile password again for confirmation.
Option button	Use this button to view the details of the selected communication profile.
Name	Name of the communication profile. The selection is required.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding a communication profile.

The system enables the following fields when you click **New** in the **Communication Profile** section.

Name	Description
Name	The name of the communication profile for the user.
Default	The profile that is made default is the active profile. There can be only one active profile at a time.

Communication Profile tab — Communication Address section

Use this section to create, modify, and delete the communication address of a user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Type	The type of the handle.
Handle	A unique communication address of the user.
Domain	The name of the domain with which the handle is registered.

Button	Description
New	The fields for adding a new communication address.
Edit	Use this button to edit the information of a selected communication address.
Delete	Deletes the selected communication address.

The page displays the following fields when you click **New** and **Edit** in the Communication Address section. The following fields define the communication address for the user.

Name	Description
Type	The type of the handle. The different types of handles are: • **Avaya SIP**: Indicates that the handle supports Avaya SIP-based communication. • **Avaya E.164**: Indicates that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. • **Microsoft OCS SIP**: Indicates that the handle supports OCS SIP-based communication. • **Microsoft Exchange**: Signifies that the handle is an e-mail address and supports communication with Microsoft SMTP server. • **Lotus Notes**: Indicates that the handle is for Lotus Notes and domino calender.

Name	Description
	• **IBM Sametime**: Indicates that the handle is for IBM Sametime. • **Avaya XMPP**: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP)-based communication with the Jabber service. • **GoogleTalk**: Indicates that the handle supports XMPP-based communication with the Google Talk service. • **Other Email**: Indicates that the handle is an e-mail address other than MS Exchange e-mail addresses. • **Other SIP**: Indicates that the handle supports other SIP-based communication than the ones mentioned above. • **Other XMPP**: Indicates that the handle supports other XMPP-based communication than the ones mentioned above.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user, or an address of an communication device using which user can send or receive messages. The selection is required.

Button	Description
Add	Saves the new communication address or modified communication address information in the database.
Cancel	Cancels the addition of communication address.

Communication Profile tab — Session Manager

Note:

The system displays the following fields only if a communication profile of the user exists for the product.

Name	Description
Primary Session Manager	Select the Session Manager instance that must be used as the home server for the currently displayed Communication Profile.

Name	Description
	As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.
Secondary Session Manager	If a secondary Session Manager instance is selected, this Session Manager provides continued service to SIP devices associated with this Communication Profile when the primary Session Manager becomes unavailable. A selection is optional.
Origination Application Sequence	Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. **Note:** If an origination and a termination application sequences are specified, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional. **Note:** If an origination and a termination application sequences are specified, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Conference Factory Set	The Conference Factory Set contains a set of Well Known Conference URIs that you can use as conference server to initiate conference calls. If the system has Conference Factory Set administered, you can get the list of Well Known Conference URIs. You require the URIs to initiate conference calls.
Survivability Server	For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a Communication Profile when the local connectivity to Session

Name	Description
	Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional. **Note:** If a termination or origination application sequence contains a Communication Manager application, Communication Manager associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.
Home Location	Specify a Home Location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any of the location. The selection is required.

Communication Profile tab — CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Name/Button	Description
System	The Communication Manager system on which you add the endpoint. The selection is required.
Profile Type	The type of the Communication Manager Endpoint profile you require to create. The selection is required.
Use Existing Endpoints	Select the check box to use the existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint that you associate this profile with. The selection is required.

Name/Button	Description
	The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Endpoint Editor button	Click to start the Communication Manager application where, you can edit or view details of the endpoint. After you save the changes in Communication Manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Template	The template, system defined or user defined, you associate with the endpoint. Select the template based on the set type you add. The selection is required.
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. The selection is required. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Provides numeric only handles, SIP or nonSIP, that are administered for a user. The **Preferred Handle** field is optional. By default the field is not set to any value. If the SIP entity is of the Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Delete Endpoint on Unassign of Endpoint from User or on Delete User	Use this check box to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.
Override Endpoint Name	Use this check box to override the following endpoint names: • The endpoint name on Communication Manager with the value you configured on

Name/Button	Description
	the Manage Users page during synchronization. If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization. • The Localized Display Name on the Manager Users page on the **Native Name** field of Communication Manager. If you clear the check box, the system does not override the Localized display name in the **Native Name** field.

Communication Profile tab — CS 1000 Endpoint Profile

Field	Description
System	The CS 1000 system on which you add a phone. The selection is required.
Target	The system customer number for the Communication Server. The selection is required.
Template	The phone or endpoint template that you can choose for the user. Select a template from the drop down list. The element manager maintains all the templates. The selection is required.
Update	Updates the station profile information for the user. When you click **Update**, the system takes you to the element manager cut through for the updates.
Service Details	Displays service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field.
Include in Corporate Directory	Use to add this profile to the CS1K Corporate Directory feature.

Communication Profile tab — Messaging Profile

Note:

The system displays the following fields only if a messaging profile can be configured for the user.

Name	Description
System	The messaging system on which you add the subscriber. The selection is required.
Use Existing Subscriber on System	Use to specify whether to use an existing subscriber mailbox number to associate with this profile.
Mailbox Number	The mailbox number of the subscriber. The selection is required. The field takes the existing mailbox number that you associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Messaging Editor button	Click to start the messaging application where, you can edit or view details of the profile of the messaging endpoint. After you save the changes in messaging, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Template	The system-defined or user-defined template you associate with the subscriber.
Password	The password for logging in to the mailbox. The selection is required.
Preferred Handle	Provides numeric only handles, SIP or nonSIP, that are administered for a user. The **Preferred Handle** field is optional. By default the field is not set to any value. If SIP entity is of Messaging type, Session Manager uses preferred handle in the Messaging Endpoint profile.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	Use to specify whether to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user.

Communication Profile tab — CallPilot Messaging Profile

Field	Description
System	The CallPilot system to which you add a mailbox. The selection is required.
Target	This field maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. The selection is required.
Template	The mailbox template you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. The selection is required.
Update	Updates the mailbox information for the user. If you click the **Update** button, the system cuts through to the element manager for the updates.
Service Details	Displays mailbox service details from endpoint after you create the mailbox.
Mailbox Number	The mailbox number or the extension DN of the user. The selection is required.

Communication Profile tab — B5800 Branch Gateway Endpoint Profile

Use this profile to assign a new or an existing user to a B5800 Branch Gateway device in user management.

While adding a user, if you have opted to assign a CM Endpoint Profile and a B5800 Branch Gateway Endpoint Profile to the user, then the B5800 Branch Gateway Endpoint Profile is used as survivability option for the CM Endpoint Profile. That is, the endpoint extension used in the CM Endpoint Profile is also used for creating a B5800 Branch Gateway Endpoint Profile so that when Communication Manager is unavailable, the B5800 Branch Gateway device can serve the extension.

Note:

If a CM Endpoint Profile is present while adding or editing a user, the user administration is considered to be in Centralized Mode, else the user administration is be considered to be in Distributed Mode.

Before you configure the B5800 Branch Gateway Endpoint Profile details, if the system has to populate the CM Endpoint Profile data or CS1000 Endpoint Profile data in the B5800 Branch Gateway Endpoint Profile fields, you must click **Commit & Continue**.

You can have a B5800 Branch Gateway Endpoint Profile as a survivable option to a CS1000 Station profile.

Name/Button	Description
System	Displays a list of B5800 Branch Gateway device names from which you can select the B5800 Branch Gateway device you associate with the user. The selection is required.
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint you associate with. The selection is required. The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Set Type	Displays the set type for the B5800 endpoint profile. By default the **Set Type** field is disabled. If you select a template, the set type gets auto populated.
Template	Displays a list of user templates from which you can select your preferred template to set the user configurations. The selection is required.
Endpoint Editor button	Starts the Avaya Aura® B5800 Branch Gateway Manager application where, you can edit or view details of the B5800 endpoint. After you save the changes in Avaya Aura® B5800 Branch Gateway Manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Delete Extension On User Delete check box	Provides the option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Membership tab — Roles section

Name	Description
check box	Use this check box to select a role. Use the check box displayed in the first column of the

Name	Description
	header row to select all the roles assigned to the user account.
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Assign Roles	Opens the Assign Role page that you can use to assign the roles to the user account.
Unassign Roles	Removes the selected role from the list of roles associated with the user account.

Membership tab — Group Membership section

Name	Description
check box	Use this check box to select a group.
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Button	Description
Add To group	Opens the Assign Groups page that you can use to add the user to a group.
Remove From Group	Removes the user from the selected group.

Contacts tab — Default Contact List

Name	Description
Description	A brief description of the contact list.

Contacts tab — Associated Contacts

Name	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Scope	Categorization of the contact based on whether the contact is a public or private contact.

Name	Description
Speed Dial	The value specifies whether the speed dial is set for the contact or not.
Speed Dial Entry	The reduced number that represents the speed dial number.
Presence Buddy	The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact.

Button	Description
Edit	Opens the Edit Contact List Member page. Use this page to modify the information of the selected contact.
Add	Opens the Attach Contacts page. Use this page to select one or more contacts from the list of contacts.
Remove	Removes one or more selected contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab — Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

Name	Description
Last Name	Last name of the private contact.
First Name	First name of the private contact.
Display Name	Display name of the private contact.
Contact Address	Address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Opens the Edit Private Contact page. Use this page to modify the information of the contact you selected.

Button	Description
New	Opens the **New Private Contact** page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Commit & Continue	Creates the user account in the database and retains you on the same page for further modifications.
Commit	Creates the user account and takes you to the User Management page.
Cancel	Cancels the user creation operation.

Related topics:

Adding a B5800 Branch Gateway endpoint profile on a user on page 308
Viewing a B5800 Branch Gateway endpoint profile of a user on page 309
Modifying a B5800 Branch Gateway endpoint profile of a user on page 309

User Profile Duplicate field descriptions

Use this page to create a duplicate user. This page has the following four tabs:

- **Identity**
- **Communication Profile**
- **Membership**
- **Contacts**

Identity tab — Identity section

Name	Description
Last Name	The last name of the user. The selection is required.
First Name	The first name of the user. The selection is required.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Login Name	The unique system log-in name given to the user. The log-in name takes the form of username@domain. You use the log-in name to create the user's primary handle. The log-in name is caseinsensitive. For example, if you enter TEST@AVAYA.COM, the system converts the log-in name to lowercase, that is, test@avaya.com. However, on the log-in page, you can enter TEST@AVAYA.COM or test@avaya.com. The log-in name can be in uppercase or lowercase. You cannot edit the **Login Name** field for users with the log-in name admin.
Authentication Type	Authentication type defines how the system performs user's authentication. The options are: • **Enterprise**: User's login is authenticated by the enterprise. • **Basic**: User's login is authenticated by an Avaya Authentication Service.
Password	Type your password for the duplicate profile.
Confirm Password	Retype your password for confirmation.
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.
Title	The personal title for address a user. This is typically a social title and not the work title.

Name	Description
Language Preference	The user's preferred written or spoken language.
Time Zone	The preferred time zone of the user.
Employee ID	The employee number for the user.
Department	The department which the user belongs to.
Company	The organization where the user works.

Identity tab — Address section

Name	Description
check box	Use this check box to select the address.
Name	The unique label that identifies the address.
Address Type	The type of address. The values are: • Office • Home
Street	The name of the street.
City	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In United States this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
New	Opens the Add Address page that you can use to add the address details.
Edit	Opens the Edit Address page that you can use to modify the address details.
Delete	Deletes the selected address.
Choose Shared Address	Opens the Choose Address page that you can use to choose a common address.

Identity tab — Localized Names section

Name	Description
Language	Specifies the localized languages for displaying the username.
Display Name	Displays the username in the localized language you choose.

Button	Description
New	Allows you to add a new localized name for the user.
Edit	Allows you to edit the localized name for the user.
Delete	Deletes the localized names you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	Cancels your add or edit of the localized name.

Button	Description
Commit	Creates the duplicate user.
Cancel	Cancels the duplicate user creation and returns to the User Management page.

Communication Profile tab — Communication Profile section

Name	Description
Option button	Use this button to view the details of the selected communication profile.
Name	Name of the communication profile.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Save	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding a communication profile.

The page displays the following fields when you click the **New** button in the Communication Profile section.

Name	Description
Name	Name of the communication profile for the user.
Default	The profile that is made default is the active profile. There can be only one active profile at a time.

Communication Profile tab — Communication Address section

Name	Description
Type	Type of the communication protocol to be used for the user.
Handle	A unique communication address for the user.
Domain	Name of the domain with which the handle is registered.

Button	Description
New	Displays the fields for adding a new communication address.
Edit	Use this button to edit the information of a selected communication address.
Delete	Deletes the selected communication address.

The page displays the following fields when you click **New** and **Edit** in the Communication Address section.

Name	Description
Type	Type of the communication protocol used for establishing communication with the user. The following are the communication protocols for the user: • **Avaya SIP**: Indicates that the handle supports SIP based communication. • **Avaya E.164**: Signifies that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. • **Microsoft Exchange**: Signifies that the handle is an e-mail address and supports

Name	Description
	communication with Microsoft SMTP server. • **Microsoft OCS SIP**: Indicates that the handle supports OCS SIP based communication. • **Lotus Notes**: Indicates that the handle is for Lotus Notes and domino calender. • **IBM Sametime**: Indicates that the handle is for IBM Sametime. • **Avaya XMPP**: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP) based communication with the Jabber service. • **Google Talk**: Indicates that the handle supports XMPP-based communication with the Google Talk service. • **Other Email**: Indicates that the handle is an e-mail address other than MS Exchange e-mail addresses. • **Other SIP**: Indicates that the handle supports other SIP-based communication than the ones mentioned above. • **Other XMPP**: Indicates that the handle supports other XMPP-based communication than the ones mentioned above.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user or of an communication device using which user can send or receive messages.

Button	Description
Add	Saves the new communication address or modified communication address information to the database.
Cancel	Cancels the adding a communication address operation.

Communication Profile tab — Session Manager

Note:

The system displays the following fields only if a communication profile of the user exists for the product.

Name	Description
Primary Session Manager	Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.
Secondary Session Manager	If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.
Origination Application Sequence	Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. **Note:** If an origination and a termination application sequences are specified, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional. **Note:** If an origination and a termination application sequences are specified, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Conference Factory Set	The Conference Factory Set contains a set of Well Known Conference URIs that you can

Name	Description
	use as conference server to initiate conference calls. If the system has Conference Factory Set administered, you can get the list of Well Known Conference URIs. You require the URIs to initiate conference calls.
Survivability Server	For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to the Communication Manager survivable remote server resident with the Branch Session Manager. A selection is optional. **Note:** If a termination or origination application sequence contains a Communication Manager application, Communication Manager associated with the application must be the main Communication Manager server for the Communication Manager survivable remote server that is resident with the Branch Session Manager.
Home Location	Specify a Home Location to support mobility for the currently displayed user. This is used by Session Manager specially in cases when the IP address of the calling phone does not match any IP Address Pattern of any of the location.

Communication Profile tab — CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Name/Button	Description
System	The Communication Manager system on which you add the endpoint. The selection is required.

Name/Button	Description
Use Existing Endpoints	Select the check box to use the existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint that you associate this profile with. The selection is required. The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Template	The template, system defined or user defined, you associate with the endpoint. Select the template based on the set type you add. The selection is required.
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. The selection is required. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Provides numeric only handles, SIP or nonSIP, that are administered for a user. The **Preferred Handle** field is optional. By default the field is not set to any value. If SIP entity is of Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Delete Endpoint on Unassign of Endpoint from User	Use this check box to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.
Override Endpoint Name	Use this check box for the following two purposes: • To override the endpoint name on Communication Manager with the value you configured on the Manage Users page during synchronization.

Name/Button	Description
	If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization. • To override the Localized Display Name on the Manager Users page on the **Native Name** field of Communication Manager. If you clear the check box, the system does not override the Localized display name in the **Native Name** field.

Communication Profile tab - CS1000 Endpoint Profile

Field	Description
System	The CS1000 system to which you want to add a phone.
Target	The system customer number for the Communication Server.
Template	The phone or endpoint template that you can choose for the user. Select a template from the drop down list. The element manager maintains all the templates.
Update	Updates the station profile information for the user. When you click this button, the system takes you to the element manager cut through for the updates.
Service Details	Displays service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field.
Include in Corporate Directory	Use to add this profile to the CS1K Corporate Directory feature.

Communication Profile tab — Messaging Profile

Note:

You may see these fields only if a messaging profile can be configured for the user.

Name	Description
System	The Messaging System on which you need to add the subscriber.
Template	The template (system defined and user defined) you want to associate with the subscriber.
Use Existing Subscriber on System	Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.
Mailbox Number	The mailbox number of the subscriber. The field lists the existing subscriber if you select the **Use Existing Subscriber on System** check box.
Password	The password for logging into the mailbox.
Delete Subscriber on Unassign of Subscriber from User	Use to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user.

Communication Profile tab - CallPilot Messaging Profile

Field	Description
System	The CallPilot system to which you want to add a mailbox.
Location	This field maps to the CallPilot Location field. This field is provided by the CallPilot Manager.
Template	The mailbox template you want to apply. Select a template from the drop down list. The element manager maintains all the mailbox templates.
Update	Updates the mailbox information for the user. If you click this button, the system cuts through to the element manager for the updates.
Service Details	Displays mailbox service details from endpoint after you create the mailbox.
Mailbox Number	Mailbox number or the extension DN of the user.

Communication Profile tab — B5800 Branch Gateway Endpoint Profile

Use this profile to assign a new or an existing user to a B5800 Branch Gateway device in user management.

While adding a user, if you have opted to assign a CM Endpoint Profile and a B5800 Branch Gateway Endpoint Profile to the user, then the B5800 Branch Gateway Endpoint Profile is used as survivability option for the CM Endpoint Profile. That is, the endpoint extension used in the CM Endpoint Profile is also used for creating a B5800 Branch Gateway Endpoint Profile so that when Communication Manager is unavailable, the B5800 Branch Gateway device can serve the extension.

Note:

If a CM Endpoint Profile is present while adding or editing a user, the user administration is considered to be in Centralized Mode, else the user administration is be considered to be in Distributed Mode.

Before you configure the B5800 Branch Gateway Endpoint Profile details, if the system has to populate the CM Endpoint Profile data or CS1000 Endpoint Profile data in the B5800 Branch Gateway Endpoint Profile fields, you must click **Commit & Continue**.

You can have a B5800 Branch Gateway Endpoint Profile as a survivable option to a CS1000 Station profile.

Name/Button	Description
System	Displays a list of B5800 Branch Gateway device names from which you can select the B5800 Branch Gateway device you want to associate with the user.
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint you want to associate. The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Set Type	Displays the set type for the B5800 endpoint profile. By default the **Set Type** field is disabled. If you select a template, the set type gets auto populated.
Template	Displays a list of user templates from which you can select your preferred template to set the user configurations.
Endpoint Editor button	Launches the Avaya Aura® B5800 Branch Gateway Manager application where, you

Name/Button	Description
	can edit or view details of the B5800 endpoint. After you save the changes in Avaya Aura® B5800 Branch Gateway Manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Delete Extension On User Delete check box	Provides the option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Membership tab — Roles section

Name	Description
check box	Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account.
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Assign Roles	Opens the Assign Role page that you can use to assign roles to the user account.
UnAssign Roles	Removes the selected role from the list of roles associated with the user account.

Membership tab — Group Membership section

Name	Description
check box	Use this check box to select the group.
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Button	Description
Add To group	Opens the Assign Groups page that you can use to add the user to a group.
Remove From Group	Removes the user from the selected group.

Contacts tab — Default Contact List

Name	Description
Name	Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name.
Description	A brief description of the contact list.

Contacts tab — Associated Contacts

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Scope	Categorization of the contact based on whether the contact is a public or private contact.
Speed Dial	The value specifies whether the speed dial is set for the contact or not.
Speed Dial Entry	The reduced number that represents the speed dial number.
Presence Buddy	The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact.

Button	Description
Edit	Opens the Edit Contact List Member page. Use this page to modify the information of the selected contact.
Add	Opens the Attach Contacts page. Use this page to select one or more contacts from the list of contacts.
Remove	Removes one or more contacts from the list of the associated contacts.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab — Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

Name	Description
Last Name	Last name of the private contact.
First Name	First name of the private contact.
Display Name	Display name of the private contact.
Contact Address	Address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Opens the Edit Private Contact page. Use this page to modify the information of the selected contact.
New	Opens the New Private Contact page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Commit & Continue	Duplicates the user account and retains you on the same page for further modifications.

Button	Description
Commit	Duplicates the user account and takes you to the User Management page.
Cancel	Cancels the operation of modifying the user information and takes you back to the User Management page.

User Delete Confirmation field descriptions

Use this page to delete an user account.

Name	Description
Last Name	Displays the last name of the user.
First Name	Displays the first name of the user.
Display Name	Displays the localized display name of a user. It is typically the localized full name.
Login Name	Displays the login name of the you want to delete.
Last login	Displays the date and time of last successful login on to System Manager.

Button	Description
Delete	Deletes a user.
Cancel	Closes the User Delete Confirmation page and takes you back to the User Management page.

Assign Roles to Multiple Users field descriptions

Use this page to assign roles to multiple users. The page has the following two sections:

- Selected Users
- Select Roles

Selected Users

Name	Description
Last Name	Displays the last name of the user.

Name	Description
First Name	Displays the first name of the user.
Display Name	Displays the localized display name of the user.
User Name	Displays the unique name that gives access to the system .
Last login	Displays the time and date when the user has logged in to the system.

Select Roles

Name	Description
Select Check box	Provides the option to select a role.
Name	Displays the name of the role.
Description	Displays a brief description about the role.

Button	Description
Commit	Assigns roles to the selected users.
Cancel	Cancels the role assignment operation and takes you back to the User Management page.

Assign Roles field descriptions

Use this page to assign a role to the user. The page has the following two sections:

- Selected Roles
- Available Roles

Selected Roles

The table in this section displays roles that you have assigned to the user account.

Name	Description
Name	Displays the roles that you have assigned to the user account.
Description	Displays a brief description about the roles.

Available Roles

The table in this section displays roles that you can assign to the user account.

Name	Description
Select check box	Provides the option to select all the roles in the table.
Name	Displays the roles that you can assign to the user account.
Description	Displays a brief description of the roles.

Button	Description
Select	Assigns the selected roles to the user.
Cancel	Cancels the role assignment operation and returns to the previous page.

Assign Groups field descriptions

Use this page to assign a group to the user account. The page has the following two sections:

- Selected Groups
- Available Groups

Selected Groups section

The table in this section displays groups that you have assigned to the user account.

Name	Description
Name	Displays the name of the group.
Type	Displays the group type based on the resources.
Hierarchy	Displays the position of the group in the hierarchy.
Description	Displays a brief description of the group.

Available Groups section

The table in this section displays groups that you can assign to the user account.

Name	Description
Select check box	Provides the option to select a group.
Name	Displays the name of the group.
Type	Displays the group type based on the resources.

Name	Description
Hierarchy	Displays the position of the group in the hierarchy.
Description	Displays a brief description of the group.

Button	Description
Select	Assigns the selected groups to the user.
Cancel	Cancels the group assignment operation.
Select: ALL	Selects all groups in the table.
Select: None	Clears the selection.

Assign Groups to Multiple Users field descriptions

Use this page to add users to the selected groups. This page has the following two sections:

- Selected Users
- Select Groups

Selected Users

Name	Description
Last Name	Displays the last name of the user.
First Name	Displays the first name of the user.
Display Name	Displays the localized display name of the user.
User Name	Displays the unique name that gives access to the system .
Last login	Displays the time and date when the user last logged on to the system.

Select Groups

Name	Description
Select check box	Provides the option to select a group.
Name	Displays the name of the group.
Type	Displays the group type based on the resources.

Name	Description
Hierarchy	Displays the position of the group within the groups.
Description	Displays a brief description of the group.

Button	Description
Select: All	Selects all the groups displayed in the table.
Select: None	Clears the selected check boxes.
Commit	Assigns groups to the selected users.
Cancel	Cancels the group assignment operation and takes you back to the User Management page.

Deleted Users field descriptions

You can view the users that you have deleted using the Delete feature. Use this page to view, permanently delete a user, and restore users that you have deleted.

Name	Description
Select check box	Provides the option to select a group.
Last Name	Displays the last name of the deleted user.
First Name	Displays the first name of the deleted user.
Display Name	Displays the localized display name of the deleted user.
User Name	Displays the unique name that identifies the user in the system.
Last login	Displays the time and date when the user last logged on to the system.

Button	Description
Delete	Deletes the user permanently from the database.
Restore	Restores the deleted user.
Show Regular users	Returns to the User page and displays the active users.

User Restore Confirmation field descriptions

Use this page to restore a deleted user.

Name	Description
Last Name	Displays the last name of the user.
First Name	Displays the first name of the user.
Display Name	Displays the localized display name of the user.
User Name	Displays the unique name of the user account.
Last login	Displays the date and time when the user last logged on to the system.

Button	Description
Restore	Removes the user from the list of deleted users and restores the user as an active user.
Cancel	Closes the User Restore Confirmation page and returns you back to the Deleted Users page.

Change Password field descriptions

Use this page to change the password for your account.

Name	Description
Old Password	The existing password.
New Password	The new password that you want to set.
Confirm Password	The new password that you want to set.

Button	Description
Save	Changes the password.
Cancel	Cancels the change password operation and closes the Change Password page.

Assign Users To Roles field descriptions

Use this page to assign one or more users to the selected roles. This page has the following two sections:

- Selected Roles
- Select Users

Selected Roles section

The roles to which you can assign users.

Name	Description
Name	Displays the name of the role.
Resource Type	Displays the resource type that the corresponding role is assigned.
Description	Displays a brief description about role.

Select Users section

The table displays the users to which you can assign the roles.

Name	Description
Select check box	Provides the option to select the user.
Last Name	Displays the last name of the user.
First Name	Displays the first name of the user.
Display Name	The display name of the user.
User Name	Displays the unique name that identifies the user.
Last Login	Displays the time and date when the user last logged on to the system.

Button	Description
Commit	Assigns user to the role.
Cancel	Cancels the assign users operation and returns to the Manage Roles page.

UnAssign Roles field descriptions

Use this page to unassign a role form the selected users. This page has the following two sections:

- Selected Roles
- Select Users

Selected Roles section

The role from which users are unassigned.

Name	Description
Name	Displays the name of the role.
Resource Type	Displays the resource type that the corresponding role is assigned.
Description	Displays a brief description about role.

Select Users section

The table displays the users for which you can remove the roles.

Name	Description
Select check box	Provides the option to select the user.
Last Name	Displays the last name of the user.
First Name	Displays the first name of the user.
Display Name	The display name of the user.
User Name	Displays the unique name that identifies the user.
Last Login	Displays the time and date when the user last logged on to the system.

Button	Description
Commit	Unassigns the role from the users.
Cancel	Cancels the assign users operation and returns to the Manage Roles page.

Managing public contacts

Manage public contact list

An administrator defines public contacts for the users in System Manager. You can share the public contacts by all the users in System Manager.

A user with administrator permission can only add, modify and delete a public contact. While creating a public contact, you need to specify the details of contact that also includes the postal address and communication address of the public contact.

The public contacts defined in the system are the default public contacts for the users and access control list.

Adding a new public contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, click **New**.
4. On the New Public Contact page, in the Contact Details section, enter the appropriate information in the respective fields.

   Fields marked with asterisk (*) are mandatory. You must enter valid information in these fields to successfully create a new public contact.

   The localized display name must be a unique name. If you do not enter any information in the **Localized Display Name** field, the system automatically generates a localized display name for the public contact.
5. In the Postal Address section, click the **New** button to add postal address of the contact .
6. In the Contact Address section, click the **New** button to add contact address.

   A contact address can be a phone number or any communication address that is supported by the application.
7. Click **Commit** to create a new public contact.

Related topics:

New Public Contact field descriptions on page 410

Modifying details of a public contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, click **Edit**.

4. On the Edit Public Contact page, modify the contact's information.
5. Click **Commit**.

Note:

Before you click **Commit**, ensure that you have entered valid information in the mandatory fields marked with an asterisk.

Related topics:

Edit Public Contact field descriptions on page 407

Deleting public contacts

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select one or more contacts.
4. Click **Delete**.
5. On the Contact Delete Confirmation page, click **Delete**.
   When you delete a public contact, the system deletes the contact from the default contact list.

Viewing the details of a public contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select a public contact and click **View**.

Result

The View Public Contact page displays the details of a public contact.

Related topics:

View Public Contact field descriptions on page 406

Adding a postal address of a public contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, perform one of the following steps:
   - If you are adding a postal address to a new public contact, click **New**.
   - If you are adding a postal address to an existing public contact, select a public contact and click **Edit**.
4. Click **New** in the Postal Address section.
5. On the Add Address page, enter the appropriate information in the respective fields.

   The fields marked with an asterisk are mandatory. You must enter a valid information in these fields.
6. Click **Add** to create a new postal address for the public contact.
7. On the New Public Contact or Edit Public Contact page, click **Commit**.

Related topics:

Add Address field descriptions on page 99

Modifying postal address of a public contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select a public contact and click **Edit**.
4. On the Edit Public Contact page, select an address from the Postal Address section.
5. Click **Edit**.
6. On the Edit Address page, modify the information in the respective fields.

   The fields marked with an asterisk are mandatory. You must enter valid information in these fields.

7. Click **Add** to save the modified address.

Related topics:

Add Address field descriptions on page 99

Deleting postal addresses of a public contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select a public contact and click **Edit**.
   If you are on the New Public Contact page, follow step 4.
4. Select a address from the table in the Postal Address section, and click **Delete**.
5. Click **Commit** to save the changes.

Choosing a shared address for a public contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. Click **Choose Shared Address**.
4. On the Choose Address page, select one or more shared addresses.
5. Click **Select** to add the selected addresses for the public contact.
6. Click **Commit**.

Adding a contact address of a public contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.

3. Click **New** in the Contact Address section.
4. On the Add Address page, enter the appropriate information in the respective fields.

   The fields marked with an asterisk are mandatory. You must enter a valid information in these fields.
5. Click **Add** to create a new contact address for the public contact.
6. On the New Public Contact page, click **Commit**.

Related topics:

Add Address field descriptions on page 331

Modifying the details of a public contact

About this task

You can use this feature to modify the contact details, postal address, and contact address of an existing public contact.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select a public contact and click **Edit**.
4. On the Edit Public Contact page, modify the information in the Contact Details, Postal Address, and Contact Address sections.

   In the Postal Address and Contact Address section you can add, modify, and delete addresses in the respective sections.

   The fields marked with an asterisk are mandatory. You must enter a valid information in these fields.
5. Click **Commit**.

Related topics:

Edit Address field descriptions on page 332

Deleting contact addresses of a public contact

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select a public contact and click **Edit**.
   If you are on the New Public Contact page, follow Step 4.
4. Select one or more addresses from the table in the Contact Address section and click **Delete**.
5. Click **Commit** to save the changes.

Add Address field descriptions

Use this page to add the mailing address of the user.

Field	Description
Address Name	Displays the unique label that identifies the mailing address.
Address Type	Displays the mailing address type such as home or office address.
Building	Displays the name of the building.
Room	Displays the number or name of the room.
Street	Displays the name of the street.
City	Displays the name of the city or town.
State or Province	Displays the full name of the province.
Postal Code	Displays the postal code or zip code used by postal services to route mail to a destination. In the United States, this is Zip code.
Country	Displays the name of the country.

Phone Details section

Field	Description
Business Phone	Displays the business phone number of the user.
Other Business Phone	Displays the secondary or alternate business phone number, if applicable.
Home Phone	Displays the residential phone number of the user.
Other Home Phone	Displays the secondary or alternate residential phone number, if applicable.
Mobile Phone	Displays the mobile number of the user.
Other Mobile Phone	Displays the secondary or alternate mobile number of the user, if applicable.
Fax	Displays the telephone number for direct reception of faxes.
Pager	Displays the number used to make calls to the user's pager.
Other Pager	Displays the secondary or alternate number used to make calls to the user's pager.

Button	Description
Add	Adds the mailing address of the user.
Cancel	Cancels the add address operation.

Related topics:

Adding a shared address on page 416
Modifying a shared address on page 417

Choose Address field descriptions

Use this page to choose a shared address for the user.

Field	Description
Name	Displays the unique label that identifies the address.
Address Type	Displays the mailing address type such as home or office address.

Field	Description
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code used by postal services to route mail to a destination. In the United States, this is Zip code.
Province	Displays the full name of the province.
Country	Displays the name of the country.

Button	Description
Select	Adds the selected mailing address as the shared contact for the user account.
Cancel	Cancels the choose address operation.

View Public Contact field descriptions

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description of the contact.
Company	Displays the name of contact's company.
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.

Postal Address

Name	Description
Name	Displays the name of the contact.

Name	Description
Address Type	Displays the mailing address type such as home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the name of the contact's company.
Province	Displays the full name of the contact's province.
Country	Displays the name of the contact's country.

Contact Address

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.
Type	Displays the type of communication medium for interacting with the user.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Related topics:

Viewing the details of a public contact on page 400

Edit Public Contact field descriptions

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.

Name	Description
Description	Displays a brief description about the contact.
Company	Displays the name of contact's company.
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.
Update Time	Displays the time when the contact information was last updated.
Source	Displays the source for provisioning the contact.

Postal Address

Name	Description
Name	Displays the name of the contact.
Address Type	Displays the mailing address type such as home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the name of the contact's company.
Province	Displays the full name of the contact's province.
Country	Displays the name of the contact's country.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to add a new postal address of the public contact.
New	Opens the **Add Address** page. Use this page to modify an existing postal address of the public contact.
Delete	Deletes the selected public contacts.

Button	Description
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the public contact.

Contact Address

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.
Type	Displays the type of communication medium for interacting with the user.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the public contact.
New	Opens the **Add Address** page. Use this page to add a contact address of the public contact.
Delete	Deletes the selected public contacts.

Button	Description
Commit	Saves the modified information to the database.

Related topics:

Modifying details of a public contact on page 399

New Public Contact field descriptions

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description of the contact.
Company	Displays the name of company.
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.

Postal Address

Name	Description
Name	Displays the name of the contact.
Address Type	Displays the mailing address type such as home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the name of the contact's company.
Province	Displays the full name of the contact's province.
Country	Displays the name of the contact's country.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to add a new postal address of the public contact.

Button	Description
New	Opens the **Add Address** page. Use this page to modify an existing postal address of the public contact.
Delete	Deletes the selected public contacts.
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the public contact.

Contact Address

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.
Type	Displays the type of communication medium for interacting with the user.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the public contact.
New	Opens the **Add Address** page. Use this page to add a contact address of the public contact.
Delete	Deletes the selected public contacts.

Button	Description
Commit	Creates a new contact. **Note:** You must enter valid information in the mandatory fields to successfully create a new contact.

Related topics:

Adding a new public contact on page 399

Public Contacts field descriptions

Use this page to add new public contacts and modify and delete existing contacts.

Public Contacts

Name	Description
Last Name	Displays the last name of the public contact.
First Name	Displays the first name of the public contact.
Display Name	Displays the display name of the public contact.
Contact Address	Displays the address of the public contact.
Description	Displays a brief description of the contact.

Button	Description
View	Open the **View Public Contact** page. Use this page to view the details of the selected public contact.
Edit	Opens the **Edit Public Contact** page. Use this page to modify the information of the selected contact.
New	Opens the **New public Contact** page. Use this page to add a new public contact.
Delete	Deletes the selected contacts.
Filter: Advanced Search	Displays fields that you can use to specify the search criteria for searching a public contact.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Criteria section

The page displays the following fields when you click **Advanced Search** . You can find the **Advanced Search** link at the at the upper-right corner of the public contact table.

Name	Description
Criteria	Displays the following three fields: • Drop-down 1– The list of criteria that you can use to search public contacts. The options are: a. Last Name: Searches public contacts by last name. b. First Name: Searches public contacts by first name. c. Display Name: Searches public contacts by display name. d. Contact Address: Searches public contacts by contact address. • Drop-down 2 – The operator for evaluating the expression. The list of operators displayed depends on the type of criterion that you have selected in drop-down 1. • Field 3 – The search value for the search criterion selected in drop-down 1.

Add Address field descriptions

Use this page to add communication address of the contact.

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, SIP, or IM of the contact. The format of the address must conform to the type of address that you select in the **Type** field.
Type	Displays the type of address. The types of addresses are: • **Phone**: This address type supports phone numbers. • **SIP**: This address type supports SIP-based communication.

Name	Description
	• **MSRTC**: This address type supports communication with a Microsoft RTC server. • **IBM Sametime**: This address type supports communication with IBM Sametime. • **XMPP**: This address type supports xmpp-based communication. • **SMTP**: This address type supports communication with the SMTP server.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Add	Adds the contact address of the public contact to the database.

Related topics:

Adding a contact address of a public contact on page 402

Edit Address field descriptions

Use this page to edit the details of a contact's communication address.

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, SIP, or IM of the contact. The format of the address must conform to the type of address that you select in the **Type** field.

Name	Description
Type	Displays the type of address. The types of addresses are: • **Phone**: This address type supports phone numbers. • **SIP**: This address type supports SIP-based communication. • **MSRTC**: This address type supports communication with a Microsoft RTC server. • **IBM Sametime**: This address type supports communication with IBM Sametime. • **XMPP**: This address type supports xmpp-based communication. • **SMTP**: This address type supports communication with the SMTP server.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Add	Saves the modified information to the database.

Related topics:

Modifying the details of a public contact on page 403

Managing shared addresses

Manage shared address

Shared address contains common addresses that you can specify for one or more users in the enterprise. The user, who is an administrator, can create a new shared address and modify

and delete an existing shared address. For example, you can add the address of the company in the list of shared address and other users can use this address as their alternative address.

Choosing a shared address

About this task

You can use this functionality to choose a shared address for a user from a set of common addresses. With this functionality, you can add, modify, and delete a shared address.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To assign shared addresses to a new user account while setting it up, click **New**.
   - To assign shared addresses to an existing user account, select a user and click **Edit**.
4. On the New User Profile page or the User Profile Edit page, click **Identity** > **Address** > **Choose Shared Address**.
5. On the Choose Address page, select one or more shared addresses.
6. Click **Select**.
7. Click **Commit**.

   When you choose a shared address for a new user, ensure that you have entered valid information in all the mandatory fields on all the tabs of the New User Profile page before you click **Commit**. If you fail to do so, the system displays an error message.

Related topics:

Choose Address field descriptions on page 102

Adding a shared address

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Shared Addresses**.

3. On the Shared Address page, click **New**.
4. On the Add Address page, enter the appropriate information.
5. Click **Add**.

Result

The new address is available as shared address and you can specify this address when you create or modify a user account.

Modifying a shared address

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Shared Addresses**.
3. On the Shared Address page, select an address and click **Edit**.
4. On the Edit Address page, modify the information in the fields.
5. Click **Add**.

Deleting a shared address

About this task

You can use this feature to delete a shared address. You cannot delete a shared address if the address is associated with one or more users.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **Shared Addresses**.
3. On the Shared Address page, select the address you want to delete and click **Delete**.

Add Address field descriptions

Use this page to add the mailing address of the user.

Field	Description
Address Name	Displays the unique label that identifies the mailing address.
Address Type	Displays the mailing address type such as home or office address.
Building	Displays the name of the building.
Room	Displays the number or name of the room.
Street	Displays the name of the street.
City	Displays the name of the city or town.
State or Province	Displays the full name of the province.
Postal Code	Displays the postal code or zip code used by postal services to route mail to a destination. In the United States, this is Zip code.
Country	Displays the name of the country.

Phone Details section

Field	Description
Business Phone	Displays the business phone number of the user.
Other Business Phone	Displays the secondary or alternate business phone number, if applicable.
Home Phone	Displays the residential phone number of the user.
Other Home Phone	Displays the secondary or alternate residential phone number, if applicable.
Mobile Phone	Displays the mobile number of the user.
Other Mobile Phone	Displays the secondary or alternate mobile number of the user, if applicable.
Fax	Displays the telephone number for direct reception of faxes.
Pager	Displays the number used to make calls to the user’s pager.
Other Pager	Displays the secondary or alternate number used to make calls to the user’s pager.

Button	Description
Add	Adds the mailing address of the user.

Button	Description
Cancel	Cancels the add address operation.

Related topics:

Adding a shared address on page 416
Modifying a shared address on page 417

Shared Address field descriptions

Use this page to create a new shared address and modify and delete an existing shared address.

Shared Address

Name	Description
Select check box	Provides the option to select an address.
Name	Displays the name of the person or entity associated with the address.
Address Type	Displays the type of address indicates whether the address is an Office or home address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code used by postal services to route mail to a destination. In the United States, this is the Zip code.
Province	Displays the full name of the province.
Country	Displays the name of the country.
Refresh	Refreshes the address information in the table.
All	Selects all the addresses in the table.
None	Clears the check box selections.

Button	Description
New	Opens the Add Address page . Use this page to add an address.
Edit	Opens the Edit Address page. Use this page to modify the mailing address information.

Button	Description
Delete	Deletes a selected address.

Managing presence access control lists

Manage Presence Access Control Lists (ACL)

You can create the following rules:

Enforced User ACL

Enforced User ACL rules define the access of presence information between individual presentities and watchers. These rules can only be set by a user who is an administrator. You can set the Enforced User ACL rules with different priorities. The rules with higher priority take precedence over the rules with lower priority.

System ACL

System ACL rules provide critical system services with a privileged access to presence of all users. System ACL rules are set at enterprise level that grant or deny a watcher the permission to view presence of all the users in the enterprise. The list that defines System ACL rules may contain several entries and each entry corresponds to one watcher.

System Rules

System Rules define the level of presence access for everyone in the enterprise. You can define multiple System Rules applicable to all presentities and all watchers in the enterprise. System Rules enforce global policies.

Default Policy

Default Policy rules are global default rules that define access to presence information if none of the more specific rules apply. There must be atleast one System Default rule defined in the system.

Viewing details of a high priority enforced ACL rule

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, in the High Priority section of the **Enforced User ACL** tab, select a rule from the list of ACL rules.

4. Click **View**.
   The system displays the View Enforced User ACL page with the details of the ACL rule you selected.

Related topics:

View Enforced User ACL field descriptions on page 442

Modifying a high priority enforced ACL rule

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, in the High Priority section of the **Enforced User ACL** tab, select a rule from the list of high priority ACL rules.
4. Perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. On the Edit High Priority Enforced User ACL page, perform one of the following steps:
   - Click **New** and create a new access level.
   - Select an existing access level and click **Edit**.
6. Click **Commit** to save the changes.

Related topics:

Edit Enforced User ACL field descriptions on page 439

Creating a new high priority enforced ACL rule

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, in the High Priority section of the **Enforced User ACL** tab, click **New**.

4. On the New High Priority Enforced User ACL page, in the Define Policy section, click **New**.
5. Create an access level.
6. In the Select Presentity section, select presentities.
7. In the Select Watcher section, select watchers.
8. Click **Commit**.

Related topics:

New Enforced User ACL field descriptions on page 436

Deleting high priority enforced ACL rules

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, in the High Priority section of the **Enforced User ACL** tab, select one or more rules you want to delete from the list of high priority rules.
4. Click **Delete**.

Viewing details of a low priority enforced ACL rule

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, in the Low Priority section of the **Enforced User ACL** tab, select a rule from the list of ACL rules.
4. Click **View**.

Result

The View Enforced User ACL page displays the details of the selected ACL rule.

Related topics:

View Enforced User ACL field descriptions on page 442

Modifying a low priority enforced ACL rule

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, in the Low Priority section of the **Enforced User ACL** tab, select a rule from the list of ACL rules.
4. Perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. On the Edit Low Priority Enforced User ACL page, perform one of the following steps:
   - Click **New** and create a new access level.
   - Select an existing access level and click **Edit**.
6. Click **Commit** to save the changes.

Related topics:

Edit Enforced User ACL field descriptions on page 439

Creating a low priority enforced ACL rule

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, in the Low Priority section of the **Enforced User ACL** tab, select a rule from the list of ACL rules.
4. On the New Low Priority Enforced User ACL page, click **New** in the Define Policy section.
5. Create an access level.
6. In the Select Presentity section, select the presentities.

7. In the Select Watcher section, select the watchers.
8. Click **Commit**.

Related topics:

New Enforced User ACL field descriptions on page 436

Deleting low priority enforced ACL rules

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, in the Low Priority section of the **Enforced User ACL** tab, select one or more rules you want to delete from the list of low priority rules.
4. Click **Delete**.

Viewing details of a System ACL rule

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, click the **System ACL** tab.
4. In the System ACL section, select a rule from the list of System ACL rules displayed.
5. Click **View**.
   The system displays the View System ACL page with the details of the selected ACL rule.

Related topics:

View System ACL field descriptions on page 449

Modifying a System ACL rule

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, click the **System ACL** tab.
4. In the System ACL section, select a rule from the list of System ACL rules displayed.
5. Perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
6. On the Edit System ACL page, perform one of the following steps:
   - Click **New** and create a new access level.
   - Select an existing access level and click **Edit**.
7. Click **Commit** to save the changes.

Related topics:

Edit System ACL field descriptions on page 447

Creating a new System ACL rule

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, click the **System ACL** tab.
4. In the System ACL section, click **New**.
5. On the New System ACL page, click **New**.
6. In the Define Policy section, click **New** and create the access level.
7. In the Select Watcher section, select the watchers.
8. Click **Commit**.

Related topics:

New System ACL field descriptions on page 444

Deleting System ACL rules

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, click the **System ACL** tab.
4. In the System ACL section, select one or more rules you want to delete from the list of System ACL rules.
5. Click **Delete**.

Defining a new policy for Enforced User ACL rules

You can use this functionality to define a new policy for the high or low priority Enforced User ACL rules. An access level rule determines the permissions a watcher has on the presence information of a presentity. With this functionality, you can also add permissions over the presence information of a presentity for a watcher.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, click **New** in the High Priority or Low Priority section of the **Enforced User ACL** tab.

   If you want to add a new policy for an existing high or low priority Enforced User ACL rule, select a rule and click **Edit**.
4. On the New High Priority Enforced User ACL or Low Priority Enforced User ACL page, click **New** in the Define Policy section.
5. From the **Access Level** drop-down field, select an access level.
6. From the **Action** drop-down field, select an action.
7. Click **Save**.
8. Click **Commit**.

Related topics:

New Enforced User ACL field descriptions on page 436
Edit Enforced User ACL field descriptions on page 439

Modifying a policy for Enforced User ACL rules

About this task

You can use this functionality to modify an existing policy for a high or low priority Enforced User ACL rule. An access level rule determines the permissions a watcher has on the presence information of a presentity. With this functionality, you can also modify the permissions over the presence information of a presentity for a watcher.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, select a rule from the High Priority or Low Priority section of the **Enforced User ACL** tab and click **Edit**.

   If you are creating a new high or low priority Enforced User ACL rule and are on the New High Priority Enforced User ACL or Low High Priority Enforced User ACL page, follow the next step.
4. Select the access level rule that you want to modify.
5. Click **Edit**.
6. Modify the information in the respective fields.
7. Click **Save**.

Related topics:

New Enforced User ACL field descriptions on page 436
Edit Enforced User ACL field descriptions on page 439

Deleting policies for Enforced User ACL rules

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, select a rule from the High Priority or Low Priority section of the **Enforced User ACL** tab and click **Edit**.

If you are creating a new high or low priority Enforced User ACL rule and are on the New High Priority Enforced User ACL or Low High Priority Enforced User ACL page, follow the next step.

4. Select one or more policies that you want to delete.
5. Click **Delete**.

Creating a system rule

About this task

You can use this functionality to define a certain level of presence access for everyone in the enterprise.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, click the **System Rule** tab.
4. In the System Rule section, click **New**.
5. On the New System Rule page, from the **Priority** drop-down field, select a priority.
6. In the Define Policy section, create an access level.
7. Click **Commit**.

Related topics:

New System Rule field descriptions on page 450

Modifying a System rule

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, click the **System Rule** tab.
4. In the System Rule section, select a rule from the list of system rules.
5. Click **Edit**.

6. On the Edit System Rule page, in the Define Policy section, perform one of the following steps:
   - Click **New** and create a new access level.
   - Select an existing access level and click **Edit** to modify the access level.
7. Click **Commit** to save the changes.

Related topics:

Edit System Rule field descriptions on page 452

Deleting system rules

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, click the **System Rule** tab.
4. In the System Rule section, select one or more rules that you want to delete from the list of system rules.
5. Click **Delete**.

Filtering presentities

About this task

You can use this functionality to filter and view selected presentities by using the following filter criteria:

- Last Name of the presentity
- First Name of the presentity
- Display Name of the presentity
- Login Name of the presentity

You can filter presentities by applying one ore more filter criteria.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.

3. On the Presence ACL page, click **New** or **Edit** from the High or Low Priority Enforced User ACL section.
4. On the New High Priority Enforced User ACL page or Low High Priority Enforced User ACL page, click **Filter: Enable** from the Select Presentity section.
5. Select or enter the filter criteria you want to apply to the selected presentity.
6. Click **Filter:Apply**.

Searching for presentities

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, in the **Enforced User ACL** tab, click **New** in the High Priority or Low Priority sections.
4. On the Create new ACL page, click **Advanced Search** in the Select Presentity section.
5. In the **Criteria** section, select the search criteria and operator from the respective fields.
6. Enter or select the search value in the third field.
7. Click the **+** button if you want to add another search condition.

   To delete a search condition, click the **-** button. You can delete a search condition only if you have more than one search condition specified.
8. Select the **AND** or **OR** operator.

   This option appears when you add a search condition using the **+** button.
9. Click **Search**.
   The page displays the presentities based on the search criteria you set in the Select Presentity section.

Filtering watchers

About this task

You can use this functionality to filter and view the watchers you selected using the following filter criteria:

- Last name of the watcher.
- First name of the watcher.
- Contact type of the watcher. Contact types are “User” and “Public contact”.

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, perform one of the following steps:
   - In the Enforced User ACL tab, click **New** in the High Priority section.
   - In the Enforced User ACL tab, click **New** in the Low Priority section.
   - In the System ACL tab, click **New** in the System ACL section.
4. Click **Filter: Enable** from the Select Watcher section.
5. Select or enter the filter criteria you want to apply to the selected watchers.
6. Click **Filter:Apply**.

Searching for watchers

Procedure

1. On the System Manager Web Console, click **Users** > **User Management**.
2. In the left navigation pane, click **System Presence ACLs**.
3. On the Presence ACL page, click **New**.
4. On the Create new ACL page, click **Advanced Search** in the Select Watcher section.
5. Select the search criteria and operator from the respective drop down fields.
6. Enter or select the search value in the third field.
7. Click the **+** button if you want to add another search condition.

   To delete a search condition, click the **–** button. You can delete a search condition only if you specify more than one search condition.
8. Select the **AND** or **OR** operator from the drop-down field.

   This option appears when you add a search condition using the **+** button.
9. Click **Search** to find watchers for the given search conditions.

The system displays the watchers that meet the search criteria in the Select Watcher section.

Presence ACL field descriptions

Enforced User ACL

This tab displays high and low priority enforced user access control list (ACL) rules for users.

High Priority

This section displays high priority enforced user ACLs. You can add a new rule and modify and delete an existing rule for users.

Name	Description
Presentity Last Name	Displays the last name of the presentity
Presentity First Name	Displays the first name of the presentity.
Watcher Last Name	Displays the last name of the watcher.
Watcher First Name	Displays the first name of the watcher.
Watcher Type	Displays the categorization of the watcher based on whether the watcher is a public or private contact.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
View	Opens the View Enforced User ACL page. Use this page to view the high priority enforced user ACL rules set for the watchers.
Edit	Opens the Edit High Priority Enforced User ACL page. Use this page to edit a high priority enforced user ACL rule set for a watcher.
New	Opens the New High Priority Enforced User ACL page. Use this page to create a rule by adding one or more access control rules and assigning these rules to one or more watchers.

Button	Description
Delete	Deletes the selected high priority enforced user ACL rules.

Low Priority

This section displays low priority enforced user ACLs. You can add a new rule and modify and delete an existing rule for users.

Name	Description
Presentity Last Name	Displays the last name of the presentity
Presentity First Name	Displays the first name of the presentity.
Watcher Last Name	Displays the last name of the watcher.
Watcher First Name	Displays the first name of the watcher.
Watcher Type	Displays the categorization of the watcher based on whether the watcher is a public or private contact.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
View	Opens the View Enforced User ACL page. Use this page to view the low priority enforced user ACL rules set for the watchers.
Edit	Opens the Edit Low Priority Enforced User ACL page. Use this page to edit a low priority enforced user ACL rule set for a watcher.
New	Opens the New Low Priority Enforced User ACL page. Use this page to create a rule by adding one or more access control rules and assigning these rules to one or more watchers.
Delete	Deletes the selected low priority enforced user ACL rules.

System ACL

This tab displays the system ACL rules for watchers. You can add a new rule and modify and delete an existing rule for watchers.

Name	Description
Watcher Last Name	Displays the last name of the watcher.
Watcher First Name	Displays the first name of the watcher.
Display Name / Login Name	Displays the display or login name of the watcher.
Watcher Type	Displays the categorization of the watcher based on whether the watcher is a public or private contact.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
View	Opens the View System ACL page. Use this page to view the system ACL rules set for the watchers.
Edit	Opens the Edit System ACL page. Use this page to edit a system ACL rule set for a watcher.
New	Opens the New System ACL page. Use this page to create a rule by adding one or more access control rules and assigning these rules to one or more watchers.
Delete	Deletes the selected System ACL rules.

System Rule

This tab displays the system rules. You can add a new rule and modify and delete an existing system rule.

Name	Description
Priority	Displays the priority set for the rule.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Opens the Edit System rule page. Use this page to edit a system rule.

Button	Description
New	Opens the New System rule page. Use this page to create a new system rule by adding one or more access control rules.
Delete	Deletes the selected system rules.

Define Policy

You can use this section to define your personal rules for accessing your presence information by one or more watchers.

Name	Description
Select check box	Provides the option to select a rule.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Use this button to delete the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define Policy section.

Name	Description
Access Level	Displays presence information for which access control rules are set. The options are • **Telephony**: Contains telephony-related presence information for which you can set an access permission. • **All**: Contains all types of presence information for which you can set an access permission.
Action	Defines the access control permission over the presence information.

Name	Description
	The options are: • **Allow**: Provides watcher the access to presence information associated with that access level. • **Block**: Blocks the watcher's access to presence information associated with this access level. • **Confirmed**: Watcher requires confirmation from the presentities to access their presence information. • **Undefined**: Access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information to the database when you add or modify a rule for watchers.

New Enforced User ACL field descriptions

Define Policy

You can use this section to add permissions on the presentity presence information for one or more watchers.

Name	Description
Select check box	Provides the option to select a rule.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Modifies an existing rule.
New	Adds a new rule for the watchers.
Delete	Deletes the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define Policy section.

Name	Description
Access Level	Displays presence information for which access control rules are set. The options are: • **Telephony**: Contains telephony-related presence information for which you can set an access permission. • **All**: Contains all the types of presence information for which you can set an access permission.
Action	Defines the access control permission over the presence information. The options are: • **Allow**: Provides watcher the access to presence information associated with that access level. • **Block**: Blocks the watcher's access to presence information associated with this access level. • **Confirmed**: Watcher requires confirmation from the presentities to access their presence information. • **Undefined**: Access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information to the database when you add or modify a rule for watchers.

Select Presentity

Name	Description
Status	The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status.
Name	Name of the user.
User Name	Unique name that gives access to the system.

Name	Description
Last Login	Date and time when the user has successfully logged into the system.
Advanced Search	Displays fields that you can use to specify the search criteria to search for presentities.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters presentities based on the filter criteria.
Select: All	Selects all the presentities in the table.
Select: None	Clears the check box selections.
Refresh	Refreshes the presentity information in the table.

Select Watcher

Name	Description
Last Name	Displays the last name of the watcher.
First Name	Displays the first name of the watcher.
Display Name/Login Name	Displays the display or login name of the watcher
Contact Type	Identifies whether the watcher is a private or public contact.
Description	Displays a brief description about the watcher.
Advanced Search	Displays fields that you can use to specify the search criteria to search for watchers.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters watchers based on the filter criteria.
Select: All	Selects all the watchers in the table.

Name	Description
Select: None	Clears the check box selections.
Refresh	Refreshes the watcher information in the table.

The page displays the following field when you click the **Advanced Search** button above the presentity and watcher table at the upper-right corner.

Name	Description
Criteria	Use the fields to define the search criteria for searching the watchers and presentities in the database. Displays the following three fields: • Drop-down 1 – Lists the search criteria. • Drop-down 2 – The list of operators for evaluating the expression. Based on the search criterion which you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down field. • Field 3 – The value for the search criterion.

Name	Description
Commit	Creates the new enforced user ACL rule for the watchers.

Related topics:

Creating a new high priority enforced ACL rule on page 421
Creating a low priority enforced ACL rule on page 423
Defining a new policy for Enforced User ACL rules on page 426
Modifying a policy for Enforced User ACL rules on page 427

Edit Enforced User ACL field descriptions

Edit Access Level Along With Action

Name	Description
Select Check box	Provides the option to select a rule.
Access Level	Displays presence information for which access control rules are set.

Name	Description
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Use this button to delete the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define Policy section.

Name	Description
Access Level	Displays presence information for which access control rules are set. The options are: • **Telephony**: Contains telephony-related presence information for which you can set an access permission. • **All**: Contains all the presence information types for which you can set an access permission.
Action	Defines the access control permission over the presence information. The options are: • **Allow**: Provides watcher the access to presence information associated with that access level. • **Block**: Blocks the watcher's access to presence information associated with this access level. • **Confirmed**: Watcher requires confirmation from the presentities to access their presence information. • **Undefined**: Access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information to the database when you add or modify a rule for watchers.

Presentity

Name	Description
Last Name	Displays the last name of the presentity.
First Name	Displays the first name of the presentity.
Middle Name	Displays the middle name of the presentity
Description	Displays a brief description about the presentity.
Login Name	A unique system login name for users that includes the users marked as deleted. Enter the login name as username@domain. Login name is used to create the user's primary handle.
Localized Display Name	Displays the localized display name of the presentity. It is the localized full name.
Endpoint Display Name	Displays the display name that identifies the presentity for an endpoint.

Contact Address

Name	Description
Handle	Displays the unique contact address for communication with the presentity.
Handle Type	Displays the qualifier that represents the type of handle.
Sub Type	Displays the sub type that defines the format of the address for the handle
Domain	Displays the domain to which the handle belongs.

Watcher

Name	Description
Last Name	Displays the last name of the watcher.
First Name	Displays the first name of the watcher.
Middle Name	Displays the middle name of the watcher.

Name	Description
Description	Displays a brief description about the watcher.
Company	Displays the company name of the watcher.
Localized Display Name	Displays the localized display name of the watcher. It is the localized full name.
Endpoint Display Name	Displays the display name that identifies the watcher for an endpoint.

Contact Address

Name	Description
Address	Displays the contact address of the watcher.
Type	Displays the qualifier that represents the type of address.
Category	Displays the category that defines whether the address is an official or residential address.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Name	Description
Commit	Saves the changes to the database.

Related topics:

[Modifying a high priority enforced ACL rule](#) on page 421
[Modifying a low priority enforced ACL rule](#) on page 423
[Defining a new policy for Enforced User ACL rules](#) on page 426
[Modifying a policy for Enforced User ACL rules](#) on page 427

View Enforced User ACL field descriptions

View Access Level Along With Action

Name	Description
Select check box	Provides the option to select a rule.

Name	Description
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Presentity

Name	Description
Last Name	Displays the last name of the presentity.
First Name	Displays the first name of the presentity.
Middle Name	Displays the middle name of the presentity
Description	Displays a brief description about the presentity.
Login Name	A unique system login name for users that includes the users marked as deleted. Enter the login name as username@domain. Login name is used to create the user's primary handle.
Localized Display Name	Displays the localized display name of the presentity. It is the localized full name.
Endpoint Display Name	Displays the display name that identifies the presentity for an endpoint.

Contact Address

Name	Description
Handle	Unique contact address for communication with the presentity.
Handle Type	Qualifier that represents the type of handle.
Sub Type	Defines the format of the address for the handle
Domain	Domain to which the handle belongs.

Watcher

Name	Description
Last Name	Displays the last name of the watcher.
First Name	Displays the first name of the watcher.
Middle Name	Displays the middle name of the watcher.

Name	Description
Description	Displays a brief description about the watcher.
Company	Displays the company name of the watcher.
Localized Display Name	Displays the localized display name of the watcher. It is the localized full name.
Endpoint Display Name	Displays the display name that identifies the watcher for an endpoint.

Contact Address

Name	Description
Address	Contact address of the watcher.
Type	Qualifier that represents the type of address.
Category	Category defines whether the address is an official or residential address.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Name	Description
Edit	Opens the Edit High Priority Enforced User ACL page. Use this page to edit the high priority ACL for a watcher.

Related topics:

Viewing details of a high priority enforced ACL rule on page 420
Viewing details of a low priority enforced ACL rule on page 422

New System ACL field descriptions

Use this page to add enterprise wide permissions on the presence information of presentties in an enterprise and associate these permissions with the watchers.

Define Policy

You can use this section to add permissions on the presentity presence information for one or more watchers.

Name	Description
Select check box	Provides the option to select a rule.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Modifies an existing rule.
New	Adds a new rule for the watchers.
Delete	Deletes the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define Policy section.

Name	Description
Access Level	Displays presence information for which access control rules are set. The options are • **Telephony**: Contains telephony-related presence information for which you can set an access permission. • **All**: Contains all the types of presence information for which you can set an access permission.
Action	Defines the access control permission over the presence information. The options are: • **Allow**: Provides watcher the access to presence information associated with that access level. • **Block**: Blocks the watcher's access to presence information associated with this access level. • **Confirmed**: Watcher requires confirmation from the presentities to access their presence information. • **Undefined**: Access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information in the database when you add or modify a rule for watchers.

Select Watcher

Name	Description
Last Name	Displays the last name of the watcher.
First Name	Displays the first name of the watcher.
Display Name/Login Name	Displays the display or login name of the watcher.
Contact Type	Identifies whether the watcher is a private or public contact.
Description	Displays a brief description about the watcher.
Advanced Search	Displays fields that you can use to specify the search criteria to search for watchers.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters watchers based on the filter criteria.
Select: All	Selects all the watchers in the table.
Select: None	Clears the check box selections.
Refresh	Refreshes the watcher information in the table.

The page displays the following field when you click the **Advanced Search** button above the presentity and watcher table at the upper-right corner.

Name	Description
Criteria	Search criteria for searching the watchers or presentities.

Name	Description
Commit	Creates the new system ACL rule for the watchers.

Related topics:

Creating a new System ACL rule on page 425

Edit System ACL field descriptions

Edit Access Level Along With Action

Name	Description
Select check box	Provides the option to select a rule.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Use this button to delete the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define Policy section.

Name	Description
Access Level	Displays presence information for which access control rules are set. The options are: • **Telephony**: Contains telephony-related presence information for which you can set an access permission. • **All**: Contains all the types of presence information for which you can set an access permission.
Action	Defines the access control permission over the presence information.

Name	Description
	The options are: • **Allow**: Provides watcher the access to presence information associated with that access level. • **Block**: Blocks the watcher's access to presence information associated with this access level. • **Confirmed**: Watcher requires confirmation from the presentities to access their presence information. • **Undefined**: Access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information to the database when you add or modify a rule for watchers.

Watcher

You can only view information in these fields.

Name	Description
Last Name	Displays the last name of the watcher.
First Name	Displays the first name of the watcher.
Middle Name	Displays the middle name of the watcher.
Description	Displays a brief description about the watcher.
Company	Displays the company name of the watcher.
Localized Display Name	Displays a brief description about the watcher.
Endpoint Display Name	Displays the display name that identifies the watcher for an endpoint.

Contact Address

You can only view information in these fields.

Name	Description
Address	Displays the contact address of the watcher.

Name	Description
Type	Displays the qualifier that represents the type of address.
Category	Displays the category that defines whether the address is an official or residential address.
Label	Need Information
Alternative Label	Need Information

Name	Description
Commit	Saves the changes to the database.

Related topics:

Modifying a System ACL rule on page 425

View System ACL field descriptions

View Access Level Along With Action

Name	Description
Select check box	Provides the option to select a rule.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Watcher

Name	Description
Last Name	Displays the last name of the watcher.
First Name	Displays the first name of the watcher.
Middle Name	Displays the middle name of the watcher.
Description	Displays a brief description about the watcher.
Company	Displays the company name of the watcher.
Localized Display Name	Displays a brief description about the watcher.

Name	Description
Endpoint Display Name	Displays the display name that identifies the watcher for an endpoint.

Contact Address

Name	Description
Address	Displays the contact address of the watcher.
Type	Qualifier that represents the type of address.
Category	Displays the category that defines whether the address is an official or residential address.
Label	Need Information
Alternative Label	Need Information

Name	Description
Edit	Opens the Edit High Priority Enforced User ACL page. Use this page to edit the high priority ACL for a watcher.

Related topics:

Viewing details of a System ACL rule on page 424

New System Rule field descriptions

New System Rule

Use this section to set a priority for the new rule.

Name	Description
Priority	Defines a priority for the new rule. The options are: • **High** • **Low** The rule with high priority has more weight than the rule with low priority.

Define Policy

You can use this section to add permissions on the presentity presence information for one or more watchers.

Name	Description
Select Check box	Provides the option to select a rule.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Use this button to delete the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define Policy section.

Name	Description
Access Level	Displays presence information for which access control rules are set. The options are • **Telephony**: Contains telephony-related presence information for which you can set an access permission. • **All**: Contains all the types of presence information for which you can set an access permission.
Action	Defines the access control permission over the presence information. The options are: • **Allow**: Provides watcher the access to presence information associated with that access level. • **Block**: Blocks the watcher's access to presence information associated with this access level.

Name	Description
	• **Confirmed**: Watcher requires confirmation from the presentities to access their presence information. • **Undefined**: Access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information to the database when you add or modify a rule for watchers.

Name	Description
Commit	Creates the new system rule for the users.

Related topics:

Creating a system rule on page 428

Edit System Rule field descriptions

Use this page to edit a system rule.

Edit Access Level Along With Action

You can use this section to add permissions on the presentity presence information for one or more watchers.

Name	Description
Select Check box	Provides the option to select a rule.
Access Level	Displays presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Use this button to delete the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

Name	Description
Access Level	Displays presence information for which access control rules are set. The options are • **Telephony**: Contains telephony related presence information for which you can set an access permission. • **All**: Contains all the types of presence information for which you can set an access permission.
Action	Defines the access control permission over the presence information. The options are: • **Allow**: Provides watcher the access to presence information associated with that access level. • **Block**: Blocks the watcher's access to presence information associated with this access level. • **Confirmed**: Watcher requires confirmation from the presentities to access their presence information. • **Undefined**: Access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information to the database when you add or modify a rule for watchers.

Name	Description
Commit	Saves the changes to the database.

Related topics:

Modifying a System rule on page 428

Chapter 5: Managing elements

System Manager Communication Manager capabilities overview

System Manager provides a common, central administration of some of the existing IP Telephony products. This helps you to consolidate the key capabilities of the current suite of Integrated Management administration products with other Avaya Management tools on a common software platform. System Manager helps you administer Avaya Aura® Communication Manager, Communication Manager Messaging, and Modular Messaging. Some features of System Manager include:

- Endpoint management
- Template management
- Mailbox management
- Discovery management
- Element Cut Through to native administration screens

Managing Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. System Manager also allows you to directly add, edit, view, or delete these objects through **Communication Manager**.

Endpoint management

Using endpoint management you can create and manage endpoint objects and add, change, remove, and view endpoint data.

Templates

Using Templates, you can specify specific parameters of an endpoint or a subscriber once and then reuse that template for subsequent add endpoint or subscriber tasks. You can use default templates, and also add your own custom templates.

There are two categories of templates: default templates and user-defined templates. You cannot edit or delete the default templates. However, you can modify or remove user-defined templates at any time.

Subscriber management

Using Subscriber Management, you can manage, add, change, remove, and view subscriber data. Subscriber management supports Avaya Aura® Messaging, Communication Manager Messaging, and Messaging objects.

With System Manager Communication Manager capabilities, you can:

- Add Communication Manager for endpoints and Modular Messaging for subscribers to the list of managed elements.
- Create templates to simplify endpoint and subscriber management.
- Administer endpoints, subscribers, and create user profiles with communication profiles.
- Associate user profiles with the required endpoints and subscribers.

Editing the Select All attribute in a table

Procedure

1. On the System Manager Web Console, click **Services** > **Configurations**.
2. Click **Settings** > **Communication System Management** > **Configuration**.
3. On the View Profile: Configuration page, edit the value of the **Select All** attribute.

   This setting affects all the tables in the user interface.

   The default value for the **Select All** attribute is 1000. You can increase this value up to 5000.

Configuring Communication Manager user profile settings

Some Communication Manager capabilities depend on the license file available with the customers. For a successful functioning of Communication Manager capabilities, ensure that the following settings are in place:

Procedure

1. Log on to Communication Manager SAT as a customer super-user. Examples of super-users are init and craft.
2. Execute the command **`display system-parameters customer-options`**.
3. On Page 5, ensure that **Station and Trunk MSP?** is set to **y**.

4. Execute the command **duplicate user-profile***18*.
5. On Page 1, perform the following:
   a. Enter a new profile number. The profile number can range from 20 to 69.
   b. Set **Shell Access** to y.
6. On Page 31, set **station M** to **wm**.
7. Save the user profile settings.
8. Exit SAT.
9. Open CM shell and perform the following to create a new user and assign password to the new user:
   a. To create a new user, use the command **cmuseradd** <*type*> [**-C** *profile*] <*login name*>

      where,

      - <*type*> is the super-user.
      - *profile* is the profile number created in Step 5.
      - <*login name*> is the user login name.

      For example, **cmuseradd super-user -C 20 iptuser**.
   b. To assign password to the new user, use the command **cmpasswd** <*login name*>

      where, <*login name*> is the login name in step 9a. For example, **cmpasswd iptuser**.

      Note:

      You can also execute Step 9 from the **Administrator Accounts** Web page in Communication Manager SMI. The navigation path for **Administrator Accounts** Web page in Communication Manager SMI is **Administration** > **Server Maintenance** > **Security** > **Administrator Accounts**.

Registering CS 1000 or CallPilot with System Manager

Adding CallPilot to the element registry

Procedure

1. On the System Manager console, click **Users** > **Administrators**.

2. In the left navigation pane, click **Elements**.
3. On the Elements page, click **Add**.
4. On the Add New Element page, specify the following:
   - **Name**: Specify the element name of the CallPilot.
   - **Description**: Specify the element description of the CallPilot.
   - **Type**: Select the element type from the drop-down list.
5. On the Add New Element page, click **Next** and then specify the following:
   - **CallPilot Manager address**: Specify the FQDN or IP address of the CallPilot Manager.
   - **CallPilot server address**: Specify the FQDN or IP address of the CallPilot server.
   - **Administrator mailbox number**: Specify the administrator mailbox number.
   - **Administrator password**: Specify the administrator password.
6. Click **Save**.

Adding CallPilot certificate to System Manager

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. In the **Elements** section, select a managed element instance.
4. On the Manage Elements page, click **More Actions** > **Configure Trusted Certificates**.
   The system displays the certificates that are currently installed on the managed element you selected.
5. To add a CallPilot certificate, click **Add**.
6. On the Add Trusted Certificate page, in the **Select Store Type to add trusted certificate** field, click **All**.
7. To add the certificate, perform one of the following:
   - To import the certificate as PEM, click **Import as PEM Certificate**.
   - Copy the certificate from the `.CER` file to the window on the Add Trusted Certificate page.

8. Click **Commit**.

Importing users from Subscriber Manager to User Management

User data import to System Manager

The User Profile Management (UPM) service in System Manager is a single point of administration for user profile data associated with multiple Avaya products. Similarly, the Subscriber Manager service in CS 1000 UCM is a single point of administration for user profile data for Heritage Nortel products. In System Manager 6.1, the UPM and Subscriber Manager applications coexist and are part of System Manager. Element Managers use:

- UPM to manage users for Heritage Avaya products
- Subscriber Manager to manage users for Heritage Nortel products

In System Manager 6.2, Subscriber Manager is merged into UPM and is called User Management (UM). UM includes several Subscriber Manager features. With the removal of Subscriber Manager, this section provides the steps that you must perform on System Manager 6.1 and 6.2 or later to ensure that the subscriber data is successfully migrated to UM of System Manager 6.2 and later.

Prerequisites

Register CS 1000 with the preupgraded System Manager Release 6.1 primary security domain.

Moving users and accounts from Subscriber Manager to User Management involves the following key procedures:

- On System Manager Release 6.1: Preparing the Subscriber Manager user data for import to User Management. This preimport procedure copies the Subscriber Manager Universally Unique ID (UUID) of the user to another field which can be preserved during the import to User Management. After the import, you require to use the UUID to reassociate phones and mailboxes.
- On System Manager Release 6.1: Importing the Subscriber Manager user data to User Management. This procedure transfers the user data from the Subscriber Manager directory to the User Management database using LDAP synchronization.
- On System Manager Release 6. 2 and later: Performing postimport tasks that involves:
    - Exporting the users to an XML file to assign communication profile passwords in User Management and reimporting the users.

- Creating the communication profile for each user, performing profile synchronization in User Management for CS 1000 and CallPilot elements that you import.

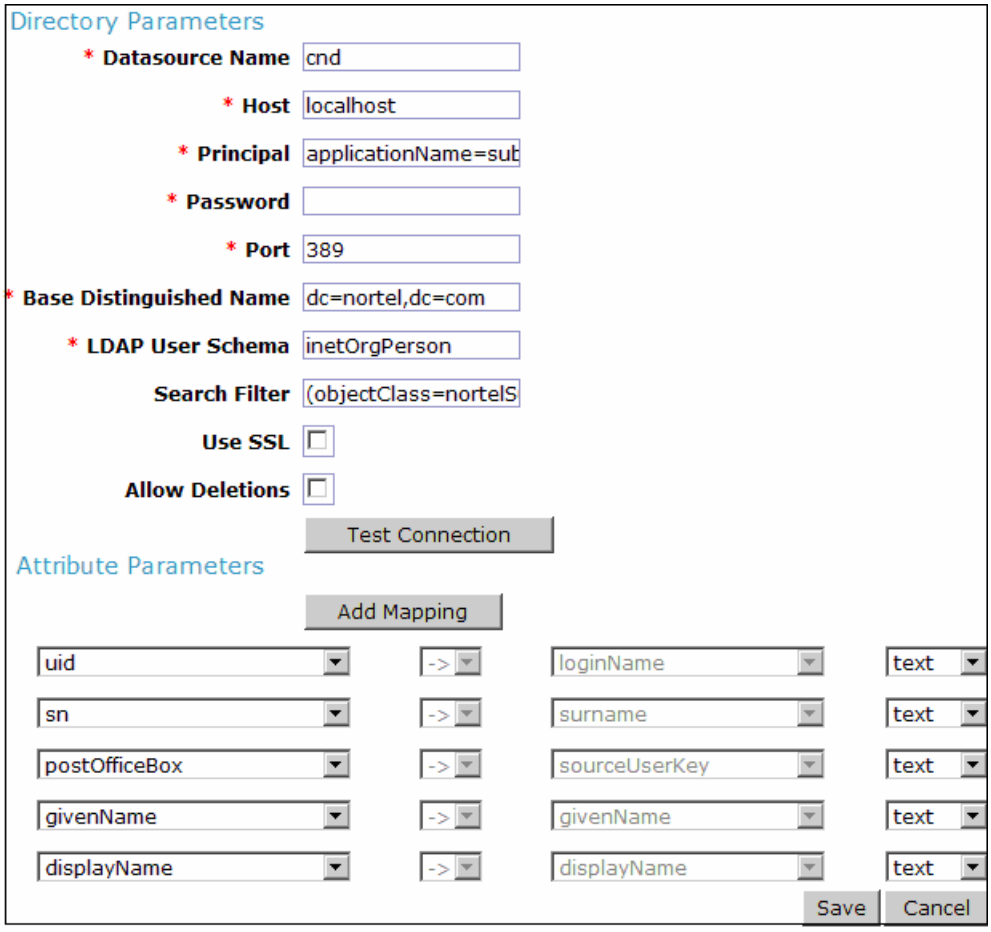
Importing the Subscriber Manager user data to User Management

Before you begin

- Log on to the Web console of System Manager Release 6.1.
- Prepare the Subscriber Manager user data for import to User Management.

Procedure

1. On System Manager Web Console, click **Users** > **Synchronize and Import**.
2. In the left navigation pane, click **Sync Users**.
3. To create a new LDAP synchronization source, on the **Synchronization Datasources** tab, click **New** and enter the directory parameters as listed in the Subscriber Manager datasource parameters and attributes table.



4. Click **Test Connection** to verify that the system can establish connection to the cnd database.
5. Perform the following steps to run the LDAP synchronization job:
   a. On the Sync Users page, on the **Active Synchronization Jobs** tab and click **Create New Job**.
   b. On the New User Synchronization Job page, in the **Datasource Name**, select the name of the datasource and click **Run Job**.

      The system starts synchronization of the Subscriber Manager datastore with the User Management datastore.
6. On the Sync Users page, on the **Synchronization Job History** tab, click **View Job Summary** for the cnd job, and verify that the system successfully imported the users in the **Added** and **Modified** fields.

   Note:

   The **Failed** field might contain some errors due to the import of unsupported fields.
7. To verify that the users are available in User Management, perform the following steps:
   a. Navigate to **Users** > **User Management** > **Manage Users**.
   b. On the User Management page, select a user and click **View** or **Edit** and verify that the System Manager Release 6.1 is configured correctly.

      System Manager Release 6.1 now contains the User Management configured with the Subscriber Manager data. The system is now ready for upgrading to System Manager Release 6.2 and later.

Subscriber Manager datasource parameters and attributes

Use the values from the following tables to update the fields on the Edit User Synchronization Datasource page.

Directory Parameters

Parameter	Value
Datasource Name	cnd
Host	For UPM: localhost For CS 1000: <**CS 1000 UCM R7.X Server IP**>
Principal	applicationName=subMgr,ou=Applications ,dc=Nortel,dc=com

Parameter	Value
Password	submgrpass
Port	389
Base Distinguished Name	dc=nortel,dc=com
LDAP User Schema	inetOrgPerson
Search Filter	(objectClass=nortelSubscriber)
Use SSL	Clear the check box.
Allow Deletions	Clear the check box.

Attribute Parameters

Map the following attributes of the Subscriber Manager datasource to the attributes of the User Management datastore.

Subscriber Manager attribute	User Management attribute	Import Type	Description
uid	loginName	text	Modified Subscriber Manager uid: user1@domain.
sn	surname	text	
postOfficeBox	sourceUserKey	text	Saved Subscriber Manager UUID.
givenName	givenName	text	
displayName	displayName	text	

Preparing the Subscriber Manager user data for import to User Management

You must perform this procedure on System Manager Release 6.1.

Before you begin

- Ensure that you install the latest CS 1000 Service Pack on all the CS 1000 Network Elements.
- Ensure that you update all Subscriber Manager user profiles for completeness that includes First Name, Last Name, and Preferred Name / CPND Name.
- Ensure that you synchronize Subscriber Manager and the CS 1000 network elements and that you upload Corporate Directory and Numbering Groups to the CS 1000 network elements.
- Ensure that the firewall is stopped on System Manager Release 6.1. Perform the following to verify that the firewall is stopped:

a. Using the command line interface, log in to System Manager Release 6.1 as `root`.

b. Enter `service iptables status`.

   The system must indicate that is stopped.

c. If firewall is enabled, enter `service iptables stop`.

   The system stops the firewall service.

Procedure

1. Log on to the Web console of System Manager Release 6.1.
2. On the Avaya Unified Communications Management page, click **Network** > **Subscriber Manager**.
3. In the left navigation pane, click **CSV Export**.
4. Click **Generate** on the upper-right of the page to create a new CSV file with the latest subscriber data.
5. Click **Download** on the upper-right of the page to download the subscriber data to your computer.

   Note the location of the `subscribers.csv` file.
6. Open the `subscribers.csv` file using Microsoft Excel and perform the following steps:

   a. Copy the data from the **UUID** column to the **postOfficeBox** column, without the column header information. This is to ensure that the Subsciber Manager datastore UUID is mapped to a column that is supported by the UPM LDAP datastore synchronization. For example:

entryUUID	postOfficeBox
c0bbc2d2-3096-4ce8-8fca-2670ea681be3	c0bbc2d2-3096-4ce8-8fca-2670ea681be3
86d11715-3b36-4238-be37-5284ca7a7a68	86d11715-3b36-4238-be37-5284ca7a7a68

   b. Copy the data from the **ucDomain** to the **User ID (uid)** column. For example:

ucDomain	uid
ca.avaya.com	user1@ca.avaya.com
ca.avaya.com	user2@ca.avaya.com

   c. Save the modified `subscribers.csv` file in a csv format.
7. To synchronize the Subscriber Manager data with the modified `subscribers.csv` file, import the modified Subscriber Manager data in the

`subscribers.csv` file back to Subscriber Manager and perform the following steps:

a. In the left navigation panel, on the **Subscriber Manager**, click **CSV Synchronization**.
b. Browse to the location where you saved the modified `subscribers.csv` file.
c. Click **Synchronize**.
d. Click **View Results** to verify that the synchronization is successful.

   If error occurs, the page displays the location of the error logs on the System Manager server. For example, `/opt/nortel/cnd/log/LDAP_Sync`.
e. Click **Subscribers**, and perform the following:

   i. Leave the **Name** field blank.

   ii. Click **Search**.
f. Select one of the user and verify that the system updated the **Unified Communication Username** field correctly.

   The system does not display the **postOfficeBox** field.

8. If Numbering Groups are used, perform the following:

a. Click **UCM Services** > **Numbering Groups**.
b. Click **Generate**.
c. Click **Export** to export the data to a location on your computer to ensure that the data is captured.

Exporting the user data and creating the user profile

To complete the import job of the user data from Subscriber Manager, you must perform the following procedure after you complete the server upgrade from System Manager Release 6.1 to Release 6.2 and later.

Before you begin

Start an SSH session.

About this task

The system does not support the export of users and user profiles in bulk from the Web console of System Manager Release 6.2 and later. Therefore, use the command line interface of System Manager to perform bulk export activities.

Procedure

1. Log in to the system, on which you require to export the user data, as `root`.
2. Export the users and the user profiles using the following steps:

a. Perform one of the following:

- For System Manager 6.3, type `cd $MGMT_HOME/bulkadministration/exportutility/`.
- For System Manager 6.2, type `$MGMT_HOME/upm/bulkexport/exportutility/`.

b. Type `sh exportUpmUsers.sh`.

The system creates an XML file `exportfile_<time stamp in milliseconds>.zip` in the `$MGMT_HOME/upm/bulkexport/` location.

The system also creates a `readme.txt` file that outlines the use and various options for the export utility in the `$MGMT_HOME/upm/bulkexport/exportutility/` directory. For information, see Bulk exporting of users.

3. Copy the zip file on the desktop of your local computer and extract the XML file.

Note the location where you saved the file.

4. Make the following edits to the XML file:

a. Add the <commPassword>password_value</commPassword> tag after the <userName> tag to assign the communication profile password in User Management.

Note:

The password must have at least 7 characters and the first character must not be a digit or a special character such as <, >, ^, %, $, @, # and *.

b. Delete the <userPassword>userpassword_value</userPassword> tag.

For example:

```
<tns:user>
        <authenticationType>enterprise</authenticationType>
        <displayName>user1</displayName>
        <displayNameAscii>user1</displayNameAscii>
        <dn>cn=f225860c-2f2c-4290-
a660-660e51fe0d4f,ou=Subscribers,dc=nortel,dc=com</dn>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>first1</givenName>
        <loginName>user1@ca.avaya.com</loginName>
        <preferredLanguage>en-US</preferredLanguage>
        <source>cnd</source>
        <sourceUserKey>c0bbc2d2-3096-4ce8-8fca-2670ea681be3</
sourceUserKey>
        <status>provisioned</status>
        <surname>last1</surname>
        <userName>user1</userName>

        <commPassword>123456</commPassword>

        <roles>
            <role>End-User</role>
        </roles>
        <ownedContactLists>
            <contactList>
                <name>list-user1_ca.avaya.com</name>
```

```
                <isPublic>false</isPublic>
                <contactListType>general</contactListType>
            </contactList>
        </ownedContactLists>
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimary>true</isPrimary>
        </commProfileSet>
    </tns:user>
```

5. Reimport the user data from the modified XML files to the Import users page on the Web console, click **Services** > **Bulk Import and Export** > **Import** > **User Management** > **Users** to go to the Import users page. For more information, see Bulk importing of users.

   Note:

   The system might display an error message when you reimport the modified user data for admin user because the XML file includes the admin user when you export the user data. Ignore the message because you cannot edit the data for the admin user.

6. To create a user profile, synchronize profile in User Management for CS 1000 or CallPilot elements that are being imported. For information on profile synchronization, see Synchronizing CS 1000 and CallPilot profiles.

   Note:

   For synchronizing the CallPilot profile, you might have to reimport the `ca.cer` file to the **Elements** > **Inventory** > **Manage Elements** page of System Manager 6.2 instead of the **UCM** > **Security** > **Certificates** page of System Manager 6.1.

Related topics:

Bulk importing of users on page 106
Bulk exporting of users on page 108
Synchronizing CS 1000 and CallPilot profiles on page 676

Importing users from CS 1000 Subscriber Manager to User Management

CS 1000 Subscriber Manager data import options

If CS 1000 Release 7.x is available while installing System Manager server 6.2 or later, you can import the CS 1000 Release 7.x Subscriber Manager user data into System Manager User Management.

Use one of the following options to import the CS 1000 Subscriber Manager data:

- Using the active primary CS 1000 Subscriber Manager server to LDAP syncnchronize the Subscriber Manager data.
- Using the CND or LDAP Data Interchange Format (LDIF) output to capture the CS 1000 Subscriber Manager data.

Preparing the CS 1000 Subscriber Manager user data for import to System Manager

This option uses the active primary CS 1000 Subscriber Manager server for System Manager User Management to perform an LDAP synchronization of the user data.

Procedure

1. Log in to the primary CS 1000 UCM server command line using one of the following user names:
   - For CS 1000 Release 7.5 systems, admin2
   - For CS 1000 Release 7.0 and later systems, nortel
2. On the CS 1000 Release 7.x UCM server, perform the steps outlined in Preparing the Subscriber Manager user data for import to User Management.

Related topics:

Preparing the Subscriber Manager user data for import to User Management on page 462

Importing the CS 1000 Subscriber Manager user data to System Manager

Before you begin

- Prepare the CS 1000 Subscriber Manager user data for import to System Manager.
- Ensure that the firewall is stopped on the CS 1000 Release 7.x server to gain access to System Manager UPM LDAP.

Procedure

1. Log on to the Web console of System Manager Release 6.2 or later.
2. Perform the LDAP synchronization as outlined in Importing the Subscriber Manager user data to User Management.

   For the directory parameters that you must use, see Subscriber Manager datasource parameters and attributes.

Related topics:

Importing the Subscriber Manager user data to User Management on page 460
Subscriber Manager datasource parameters and attributes on page 461

Exporting the CS 1000 user data and creating the user profile

To complete the import job of user data from CS 1000 Subscriber Manager:

Procedure

Perform the same procedure as System Manager Release 6.1 Exporting the user data and creating the user profile on page 464.

Related topics:

Exporting the user data and creating the user profile on page 464

Preparing the CS 1000 Subscriber Manager user data for import to System Manager

This method uses the CND or LDIF output to capture the CS 1000 Subscriber Manager user data that you later import to User Management in System Manager.

Perform this procedure on System Manager Release 6.2 or later.

Procedure

1. Log in to the primary CS 1000 UCM server command line using one of the following user names:
   - For CS 1000 Release 7.5 systems, admin2
   - For CS 1000 Release 7.0 and later systems, nortel
2. On the CS 1000 Release 7.x UCM server, perform the steps outlined in Preparing the Subscriber Manager user data for import to User Management in System Manager.
3. Change to super user su - root.
4. Type `cd /opt/nortel/cnd`.
5. Type `./cnd.sh stop_service`.
6. Type `./slapcat -f slapd.conf –s ou=subscribers,dc=nortel,dc=com –a objectclass=nortelsubscriber -l subscriberData.ldif`.
7. Type `./cnd.sh start_service`.
8. Using a secure ftp client, connect to the CS 1000 UCM Linux system using the same credentials you used in Step 1.
9. Copy the `/opt/nortel/cnd/subscriberData.ldif` file to your computer.

Related topics:

Preparing the Subscriber Manager user data for import to User Management on page 462

Importing the CS 1000 UCM Subscriber Manager user data to System Manager

Before you begin

- Prepare the CS 1000 Release 7.x Subscriber Manager user data for import to System Manager User Management.

Procedure

1. Using a secure ftp client, connect to the System Manager server using admin.
2. Copy the `subscriberData.ldif` file to the `/home/admin` directory on System Manager.
3. Log on to System Manager server using the command line interface.

4. Change to the super user su - root.
5. Type `cd /opt/nortel/cnd`.
6. Type `mv /home/admin/subscriberData.ldif`.
7. Type `./cnd.sh stop_service`.
8. Type `./slapadd -f slapd.conf -l subscriberData.ldif –c`.
9. Type `./cnd.sh start_service`.
10. Perform the LDAP synchronization procedure as outlined in Importing the Subscriber Manager user data to System Manager.

Note:

Ensure that the **Host** field in the **Directory Parameter** area displays localhost.

Exporting the CS 1000 user data and creating the user profile

To complete the import job of user data from CS 1000 Subscriber Manager:

Procedure

Perform the same procedure as System Manager Release 6.1 Exporting the user data and creating the user profile on page 464.

Related topics:

Exporting the user data and creating the user profile on page 464

B5800 Branch Gateway Manager

B5800 Branch Gateway Element Manager

Use the B5800 Branch Gateway feature in System Manager to remotely configure and manage B5800 Branch Gateway devices. Through this feature, you can also perform backup and restore tasks of B5800 Branch Gateway device configurations.

System Manager discovers B5800 Branch Gateway devices in discovery management through SNMPv1. The discovered B5800 Branch Gateway devices appear in the Collected Inventory list in **Inventory**.

System Manager provides support to launch the B5800 Branch Gateway application, the interface on which you can view or edit configuration values. JRE 6 Update 22 and above is a prerequisite in client machines for the B5800 Branch Gateway application support in System Manager.

Use the administrative capabilities of B5800 Branch Gateway in System Manager to:

- Edit and view system configuration data under **System Configuration**.
- Edit and view security configuration data under **Security Configuration**.
- Perform backup and restore tasks of B5800 Branch Gateway device configuration that includes system configuration data and user data.
- Synchronize the B5800 Branch Gateway devices through the **Inventory** tab.

Note:

When you use a B5800 Branch Gateway device through System Manager, System Manager locks the device from external access. You can unlock the device by editing the security settings in System Manager. You must edit the security settings only in critical scenarios.

To create system configuration and endpoint templates for B5800 Branch Gateway devices, use the **B5800 Endpoint** and **B5800 System Configuration** pages in template management. In addition to system configuration template creation, you can even apply a system configuration template to a B5800 Branch Gateway device. Use the **B5800 Endpoint** and **B5800 System Configuration** menus in template management in System Manager to:

- Create, edit, view, duplicate, and delete B5800 Endpoint templates.
- Create, edit, view, duplicate, and delete B5800 System Configuration templates.
- Upload and convert the audio files from .WAV to .C11 format
- Apply B5800 System Configuration templates to B5800 Branch Gateway devices.

Launching the B5800 Branch Gateway Element Manager

The B5800 Branch Gateway Element Manager application is a prerequisite for successful completion of administrative tasks on the **Security Configuration** and **System Configuration** pages under **B5800 Branch Gateway** in Elements, **B5800 Endpoint** and **B5800 System Configuration** pages under **Templates**, and the **B5800 Branch Gateway Endpoint Profile** section in User Profile Management in System Manager.

You must set up System Manager to launch the B5800 Branch Gateway Element Manager if you have newly installed System Manager, or when you are required to upgrade B5800 Branch Gateway Element Manager to the latest version available on PLDS.

Setting up System Manager to launch Avaya B5800 Branch Gateway Element Manager

Procedure

1. Download the B5800 Branch Gateway Element Manager `B5800AdminLite.exe` file from http://plds.avaya.com.
2. Transfer the downloaded `B5800AdminLite.exe` file to the System Manager server using SFTP/SCP to the directory `/opt/Avaya/ABG/<version>/tools`. For example, `/opt/Avaya/ABG/6.2.12/tools`.
3. Change this file into an executable file using the command: `chmod +x <file name>`.
4. You must create a soft link using the name *ManagerSFX.exe* for the uploaded file. Goto `$ABG_HOME/tools by doing cd $ABG_HOME/tools`, and create a soft link using the command **`ln -sf target linkname`**
   If the filename uploaded to $ABG_HOME/tools is *B5800ManagerLite.exe*, then run the **`ln -sf B5800ManagerLite.exe ManagerSFX.exe`** command.
5. Update the parameter, `abg_b5800_mgr_version`, in the `/opt/Avaya/ABG/<version>/tools/ManagerSFXVersion.properties` file with the version of B5800 Branch Gateway Element Manager you downloaded from PLDS.
6. If you have a B5800 Branch Gateway administration suite already installed on your computer using the B5800 Branch Gateway Administration Applications DVD, update the *abg_b5800_mgr_version* parameter with the manager version of your computer in the `/opt/Avaya/ABG/<version>/tools/ManagerSFXVersion.properties` file on System Manager.

   Important:

   You must update the `abg_b5800_mgr_version` parameter each time you download a new version of B5800 Branch Gateway Element Manager from PLDS and transfer to System Manager.

   Failing to do so, when you try to launch B5800 Branch Gateway Element Manager through System Manager, the launch will fail and the system displays an error message prompting you to update the parameter.
7. On the administration computer that is used to launch B5800 Branch Gateway, set the environment variable to match the version of the B5800AdminLite.exe file. Depending on the version of Windows running on your computer, do one of the following:
   - If the computer is running Windows XP, see Setting up the environment variable in Windows XP to match the version of AdminLite on page 473.

- If the computer is running Windows 7, see Setting up the environment variable in Windows 7 to match the version of AdminLite on page 476.

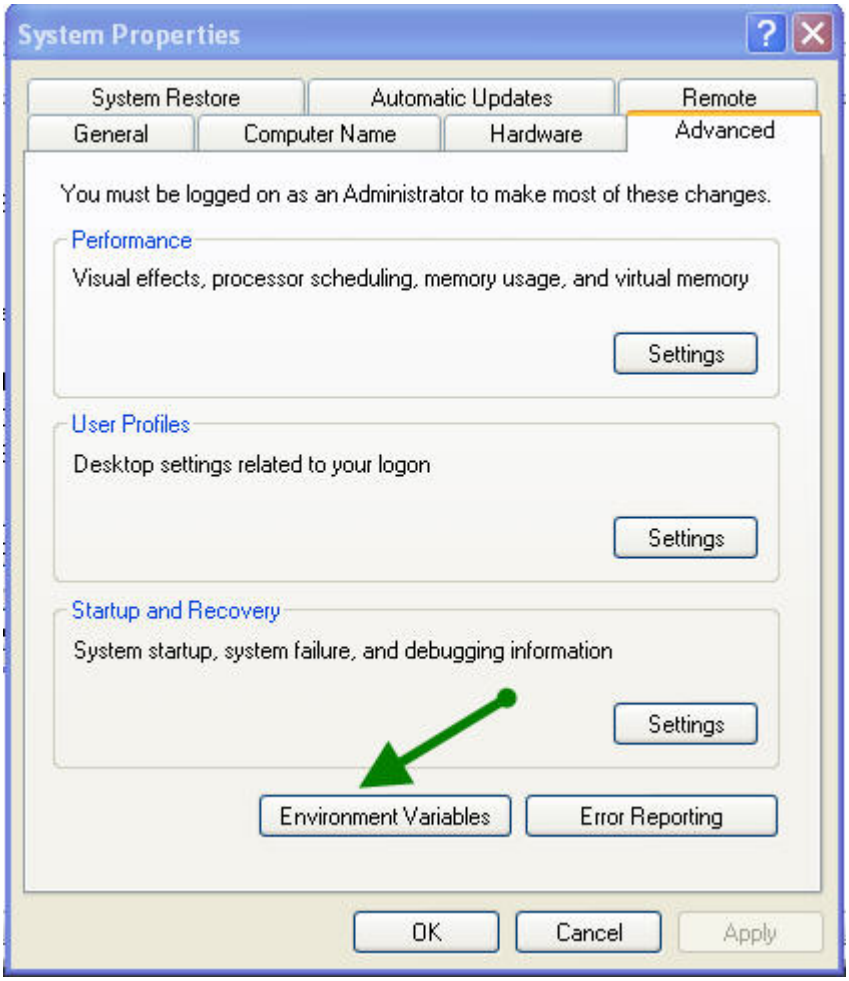
Setting up the environment variable in Windows XP to match the version of AdminLite

About this task

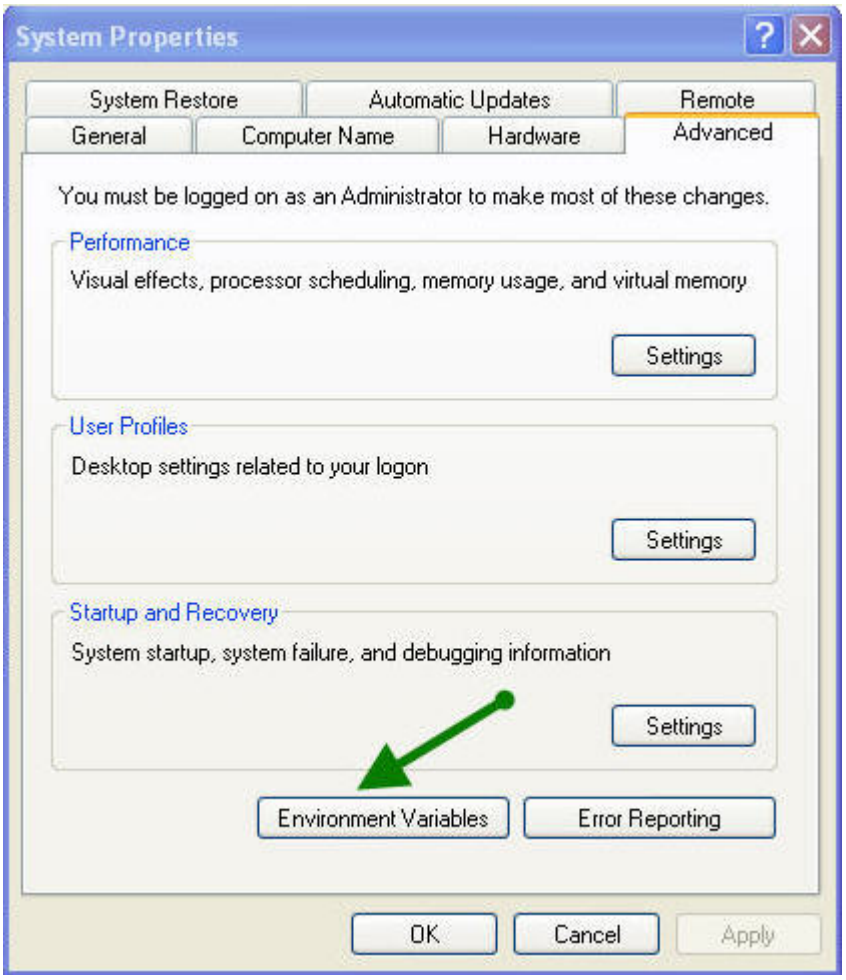
Follow this procedure to set your system's environment variable to match the version of AdminLite you install.

Procedure

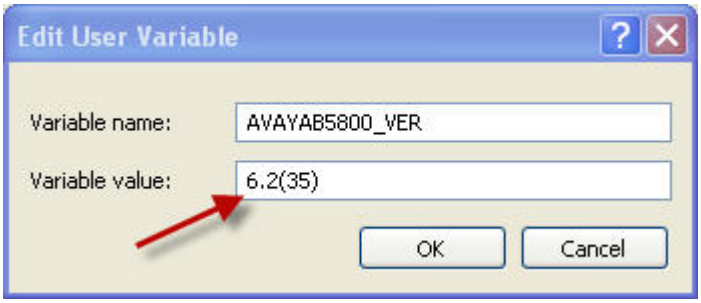
1. From the **Start** menu, right-click **My Computer**.
2. Click **Properties**.
3. In the System Properties dialog box, click the **Advanced** tab.
4. Click **Environment Variables**.



5. In the Environment Variables dialog box, in the **User variables for <name> area**, select **AVAYAB5800_VER**.
6. Click **Edit**.



7. In the Edit User Variable dialog box, in the **Variable value** field, change the value to match the version of B5800AdminLite, for example, `6.2`.



8. Click **OK**.
9. Click **OK** for each of the subsequent dialog box, and then click **Apply**.

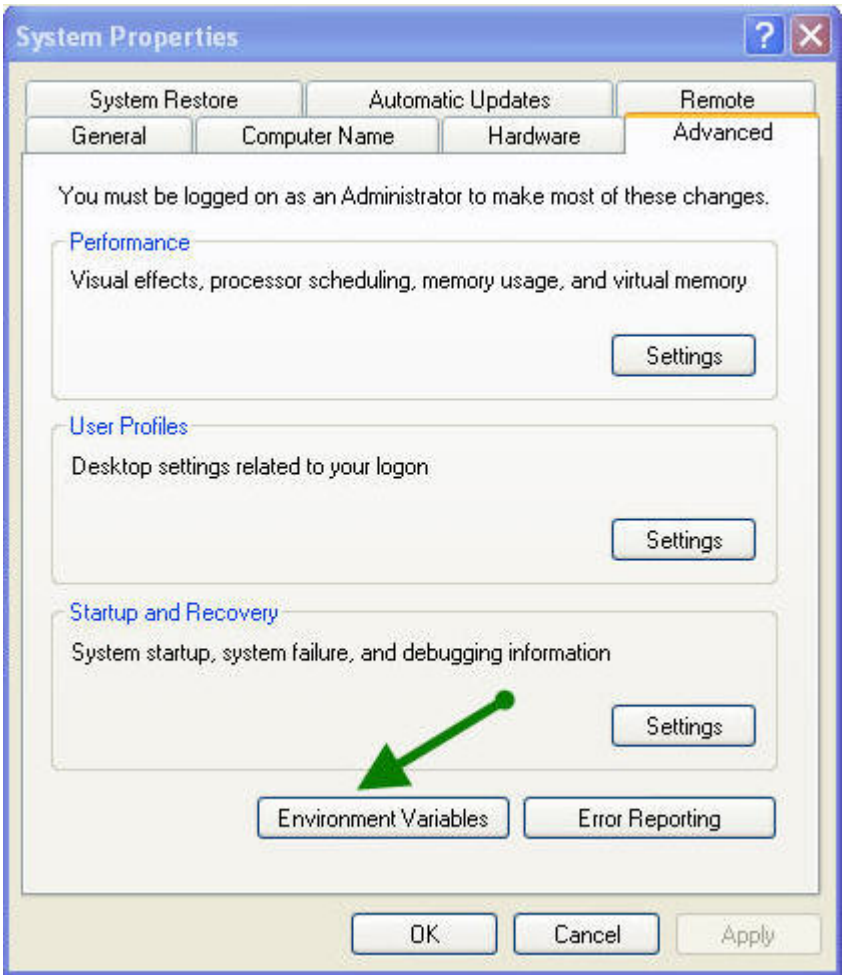
Setting up the environment variable in Windows 7 to match the version of AdminLite

About this task

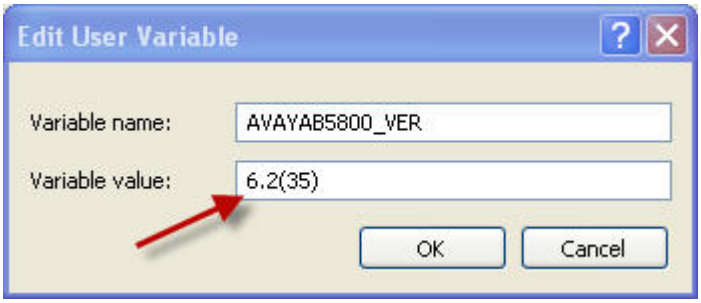
Follow this procedure to set your system's environment variable to match the version of AdminLite you install.

Procedure

1. From the **Start** menu, right-click **Computer**.
2. Click **Properties**.
3. In the left navigation pane, click **Advanced system settings**.
4. In the System Properties dialog box, click **Environment Variables**.
5. In the Environment Variable dialog box, in the **User variables for <name>** area, select **AVAYAB5800_VER**.
6. Click **Edit**.



7. In the Edit User Variables dialog box, in the **Variable value** field, change the value to match the version of B5800AdminLite, for example, `6.2`.



8. Click **OK**.
9. Click **OK** for each of the subsequent dialog box, and then click **Apply**.

Default login password for day one configuration of a B5800 Branch Gateway device

As part of day 1 configuration for a B5800 Branch Gateway device in Application Management in System Manager, you must use the default service login and password to enable the use of B5800 Branch Gateway device through System Manager. The following are the default values for the **Service Login** and **Service Password** fields under the **Attributes** tab on the New B5800 Branch Gateway page:

- **Service Login**: `SMGRB5800Admin`
- **Service Password**: `SMGRB5800Admin`

Navigation for the New B5800 Branch Gateway page in Application Management from the dashboard: **Inventory** > **Manage Elements** > **New**.

This is a one-time use service password. After you commit this service login and password, the system changes this default password internally and generates a random password. The system does not display the new password. If you want to reset the login password, you must do so by connecting locally to the B5800 Branch Gateway device using the B5800 Branch Gateway Manager.

Important:

After the password change operation, a default Sync system configuration is scheduled. A system configuration backup job is also scheduled everyday.

System Configuration

System Configuration

Use the **System Configuration** pages to view and edit system configuration of B5800 Branch Gateway devices through System Manager.

To view or edit system configuration values, you must launch the B5800 Branch Gateway Element Manager in the *offline* mode through System Manager. System Manager uses its Web services to obtain the latest system configuration from a B5800 Branch Gateway device and passes it to theB5800 Branch Gateway Element Manager. After you save the modifications on theB5800 Branch Gateway Element Manager,System Manager retrieves the modified system configuration file and pushes it to the B5800 Branch Gateway device.

Viewing a system configuration

Procedure

1. On the System Manager Web Console, click **Elements** > **B5800 Branch Gateway**.
2. In the left navigation pane, click **System Configuration**.
3. On the B5800 Branch Gateway System Configuration List page, select the B5800 Branch Gateway device whose system configuration you want to view.
4. Click **View**.
   This action launches theB5800 Branch Gateway Manager application.
5. On the Avaya B5800 Branch Gateway Manager window, you can view the details of the selected B5800 Branch Gateway system configuration on the right pane. All the fields are view only.
6. Click **File** > **Exit** to exit the B5800 Branch Gateway Manager application and return to the B5800 Branch Gateway System Configuration landing page.

Related topics:

B5800 Branch Gateway System Configuration field descriptions on page 480

Editing a system configuration

Procedure

1. On the System Manager Web Console, click **Elements** > **B5800 Branch Gateway**.
2. In the left navigation pane, click **System Configuration**.
3. On the B5800 Branch Gateway System Configuration List page, select the B5800 Branch Gateway device whose system configuration you want to edit.
4. Click **Edit**.
   This action launches theB5800 Branch Gateway Manager application.
5. On the Avaya B5800 Branch Gateway Manager window, edit the required fields on the right pane.
6. Click **File** > **Save Configuration and Exit** to save the modifications and exit the B5800 Branch Gateway Manager application.
7. On the B5800 Branch Gateway System Configuration Edit page, the system displays the selected B5800 Branch Gateway device in the device list. Perform one of the following:

- Click **Commit** to apply the changes immediately.
- Click **Schedule** to apply the changes at a specified time.

Related topics:

B5800 Branch Gateway System Configuration field descriptions on page 480

B5800 Branch Gateway System Configuration field descriptions

Name	Description
Device Name	Displays the name of the B5800 Branch Gateway device.
IP Address	Displays the IP address associated with the B5800 Branch Gateway device.
System Type	Displays the type of system associated with the B5800 Branch Gateway device. The valid options are: • **B5800**: for Core Unit • **B5800L**: for Linux systems
Last Operation on Device	Displays the operation that has been performed last on the device.
Status	Specifies the status of the operation that is currently running or was last run.
System Configuration Template	Displays the current B5800 System Configuration template that exists on the B5800 Branch Gateway device.
Last Modified Time of System Configuration	Displays the date and time you last modified the system configuration.
Last Backup Time	Displays the date and time when you last performed a backup.

Security Configuration

Security Configuration

Use the **Security Configuration** pages to view and edit the security configuration values of B5800 Branch Gateway devices through System Manager.

To view or edit security configuration values, you must launch the B5800 Branch Gateway in*online* mode through System Manager. System Manager uses its Web services to obtain the latest security configuration from a B5800 Branch Gateway device and passes it to theB5800 Branch Gateway Element Manager. After you save the modifications on the B5800 Branch Gateway Element Manager, System Manager retrieves the modified security configuration file and pushes it to the B5800 Branch Gateway device. After the security configuration files are successfully uploaded to the device, System Manager deletes the local copy of these security configuration files.

Viewing a security configuration

Procedure

1. On the System Manager Web Console, click **Elements** > **B5800 Branch Gateway**.
2. In the left navigation pane, click **Security Configuration**.
3. On the B5800 Branch Gateway Security Configuration List page, select the B5800 Branch Gateway device whose Security Configuration you want to view.
4. Click **View**.
   This action launches theB5800 Branch Gateway Manager application.
5. On the B5800 Branch Gateway Manager window, you can view the details of the selected B5800 Branch Gateway Security Configuration on the right pane. All the fields are view only.
6. Click **File** > **Exit** to exit the B5800 Branch Gateway Manager application and return to the B5800 Branch Gateway Security Configuration landing page.

Related topics:

B5800 Branch Gateway field descriptions on page 482

Editing a security configuration

Procedure

1. On the System Manager Web Console, click **Elements** > **B5800 Branch Gateway**.
2. In the left navigation pane, click **Security Configuration**.
3. On the B5800 Branch Gateway Security Configuration List page, select the device whose security configuration you want to edit.
4. Click **Edit**.
   This action launches theB5800 Branch Gateway Manager application.

5. On the B5800 Branch Gateway Manager window, edit the required fields on the right pane.
6. Click **File** > **Save Security Settings and Exit** to save the modifications and exit the B5800 Branch Gateway Manager application.

   The system directs you to the B5800 Branch Gateway Security Configuration landing page.

   After you save the configuration, System Manager retrieves the edited security configuration file from B5800 Branch Gateway Manager application and pushes it to the B5800 Branch Gateway device.

Related topics:

B5800 Branch Gateway field descriptions on page 482

B5800 Branch Gateway field descriptions

Device list

Name	Description
Device Name	Displays the name of the B5800 Branch Gateway device.
IP Address	Displays the IP address associated with the B5800 Branch Gateway device.
System Type	Displays the type of system associated with the B5800 Branch Gateway device. The valid options are: • **B5800**: for Core Unit • **B5800L**: for Linux systems
Last Operation on Device	Displays the last operation that you perform on the device.
Status	Specifies the status of the operation that is currently running or was last run.
System Configuration Template	Displays the current B5800 System Configuration template that exists on the B5800 Branch Gateway device.
Last Modified Time of System Configuration	Displays the date and time when you the system configuration operation was last carried out.

Name	Description
Last BackupTime	Displays the date and time you last performed the backup activity on the B5800 Branch Gateway device.

Backup and restore of B5800 Branch Gateway device configuration

Backup and restore of B5800 Branch Gateway device configuration

Use the **Backup and Restore** feature under **Elements** > **B5800 Branch Gateway**in System Manager to perform the backup and restore tasks of the B5800 Branch Gateway device configuration from the **B5800 Branch Gateway Backup** and **B5800 Branch Gateway Restore** pages. A B5800 Branch Gateway device configuration contains system configuration data and user data.

The **B5800 Branch Gateway Backup** pages provide you the option to create a local backup where the system stores the backup output on the local storage attached to the B5800 Branch Gateway device. The B5800 Branch Gateway device stores only one copy of the backup file at any given point of time on the local storage.

You can choose to perform the backup and restore tasks on demand or schedule it for a specified time. You can also modify the scheduled job time from the **Scheduler** service in System Manager. You can view the logs of the backup and restore tasks on the Log Harvesting pages in System Manager.

Creating a backup of the B5800 Branch Gateway device configuration

Procedure

1. On the System Manager Web Console, click **Elements** > **B5800 Branch Gateway**.
2. In the left navigation pane, click **Backup and Restore**.
3. On the B5800 Branch Gateway Backup page, select the B5800 Branch Gateway device from the List of Device for which you want to create a backup.
4. Click **Backup**.

   The B5800 Branch Gateway device you selected is listed under the **Device List**.
5. Click **Now** to perform the backup task immediately, or perform one of the following:
   - Click **Schedule** to perform the backup task at a specified time.
   - Click **Cancel** to cancel the backup task.

You can view the status of the backup task for the device you selected using the **Status** button.

Related topics:

Backup and Restore field descriptions on page 485

Restoring the B5800 Branch Gateway device configuration

Procedure

1. On the System Manager Web Console, click **Elements** > **B5800 Branch Gateway**.
2. In the left navigation pane, click **Backup and Restore**.
3. On the B5800 Branch Gateway Backup page, select the B5800 Branch Gateway device from the List of Device whose backed up configuration you want to restore. You can also select multiple devices.
4. Click **Restore**.
5. The B5800 Branch Gateway device you selected is listed under **Device List**. In **Restore Options**, perform one of the following:
   - Select **System Configuration** to restore the respective system configurations available in System Manager on to the B5800 Branch Gateway device. The configuration you restore is the latest configuration available in System Manager.
   - Select **User** to restore the respective users from System Manager on to the B5800 Branch Gateway device.
   - Select **System Configuration And User** to restore the respective system configurations and users from System Manager on to the B5800 Branch Gateway device.
   - Select **Restore Backup Stored on Devices** to restore the locally backed up configuration on to the B5800 Branch Gateway device.
6. Click **Now** to perform the restore activity immediately or perform one of the following:
   - Click **Schedule** to perform the restore activity at a specified time.
   - Click **Cancel** to cancel the restore activity.

   You can view the status of the restore job in the **Scheduler** service.

Related topics:

Backup and Restore field descriptions on page 485

Backup and Restore field descriptions

B5800 Branch Gateway Backup page device list

Name	Description
Device Name	Displays the name of the B5800 Branch Gateway device.
IP Address	Displays the IP address associated with the B5800 Branch Gateway device.
System Type	Displays the type of system associated with the B5800 Branch Gateway device. The valid options are: • **B5800**: for Core Unit • **B5800L**: for Linux systems
Version	Displays the version number of the B5800 Branch Gateway device.
System Configuration Template	Displays the current B5800 System Configuration template that exists on the B5800 Branch Gateway device.

B5800 Branch Gateway Restore page device list

Name	Description
Device Name	Displays the name of the B5800 Branch Gateway device.
IP Address	Displays the IP address associated with the B5800 Branch Gateway device.
System Type	Displays the type of system associated with the B5800 Branch Gateway device. The valid options are: • **B5800**: for Core Unit • **B5800L**: for Linux systems
Version	Displays the version number of the B5800 Branch Gateway device.
System Configuration Template	Displays the current B5800 System Configuration template that exists on the B5800 Branch Gateway device.
Restore Options	Provides options for restoring backed up configuration that is stored either on System

Name	Description
	Manager or on the B5800 Branch Gateway device. • **System Configuration**: Restores the latest configuration available onSystem Manager • **User**: Restores users stored on System Manager • **System Configuration And User**: Restores the backed up system configuration and users stored on System Manager • **Restore Backup Stored on Devices**: Restores the locally backed up configuration

Button	Description
Backup	Opens the **B5800 Branch Gateway Backup** page. Use this page to create a local backup in the B5800 Branch Gateway device.
Restore	Opens the **B5800 Branch Gateway Restore** page. Use this page to restore backed up system configuration to a B5800 Branch Gateway device.
Status	Specifies the status of the operation that is currently running or was last run.
Now	Performs the backup or restore job, as applicable, immediately.
Schedule	Opens the **B5800 Branch Gateway Job Scheduler** page. Use this page to schedule a backup.
Cancel	Cancels the backup or restore job, as applicable, and directs you to the **Backup and Restore** landing page.

B5800 Branch Gateway field descriptions

Device list

Name	Description
Device Name	Displays the name of the B5800 Branch Gateway device.
IP Address	Displays the IP address associated with the B5800 Branch Gateway device.
System Type	Displays the type of system associated with the B5800 Branch Gateway device. The valid options are: • **B5800**: for Core Unit • **B5800L**: for Linux systems
Last Operation on Device	Displays the last operation that you perform on the device.
Status	Specifies the status of the operation that is currently running or was last run.
System Configuration Template	Displays the current B5800 System Configuration template that exists on the B5800 Branch Gateway device.
Last Modified Time of System Configuration	Displays the date and time when you the system configuration operation was last carried out.
Last BackupTime	Displays the date and time you last performed the backup activity on the B5800 Branch Gateway device.

Managing Communication Manager objects

Communication Manager objects

Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. Through **Communication Manager** you can directly add, edit, view, or delete the Communication Manager objects. These objects are:

Group	Communication Manager objects
Call Center	Agents Announcements Audio Group Best Service Routing Holiday Tables Variables Vector Vector Directory Number Vector Routing Table Service Hours Tables
Coverage	Coverage Answer Group Coverage Path Coverage Remote Coverage Time of Day
Endpoints	Alias Endpoint Intra Switch CDR Manage Endpoints Off PBX Endpoint Mapping Site Data Xmobile Configuration
Groups	Group Page Hunt Group Intercom Group Pickup Group Terminating Extension Group
Network	Automatic Alternate Routing Analysis Automatic Alternate Routing Digit Conversion

	Automatic Route Selection Analysis Automatic Route Selection Digit Conversion Automatic Route Selection Toll Data Modules IP Interfaces IP Network Regions Node Names Route Pattern Signaling Groups Trunk Group
Parameters	System Parameters - CDR Options System Parameters - Customer Options System Parameters - Features System Parameters - Security System Parameters - Special Applications
System	Abbreviated Dialing Enhanced Abbreviated Dialing Group Abbreviated Dialing Personal Authorization Code Class of Restriction Class of Service Class of Service Group Dialplan Analysis Dialplan Parameters Feature Access Codes Locations Uniform Dial Plan Uniform Dial Plan Group

Note:

You cannot add, edit, or delete Audio Groups, Announcements, Subscribers, and Class of Service objects through Element Cut Through.

Related topics:

[Adding Communication Manager objects](#) on page 490
[Editing Communication Manager objects](#) on page 490
[Viewing Communication Manager objects](#) on page 491
[Deleting Communication Manager objects](#) on page 491
[Filtering Communication Manager objects](#) on page 492

Adding Communication Manager objects

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Select the Communication Manager again from the list of Communication Managers.

   Note:

   Enter the qualifier number in the **Enter Qualifier** field, if applicable.
7. Click **Add**.
   The system displays the Element Cut Through screen where you can enter the attributes of the Communication Manager object you want to add.
8. Click **Enter** to add the Communication Manager object.
   To return to the Communication Manager screen, click **Cancel**.

Editing Communication Manager objects

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the group list, select the device you want to edit.
6. Click **Edit**.
   The system displays the Element Cut Through screen where you can edit the attributes of the device you have chosen.
7. To save the changes and go back to the Communication Manager screen, click **Enter**.

To undo the changes and return to the Communication Manager screen, click **Cancel**.

Viewing Communication Manager objects

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the group list, select the object you want to view.
6. Click **View**.
   You can view the attributes of the object you have selected in the Element Cut Through screen.
7. To return to the Communication Manager screen, click **Cancel**.

Deleting Communication Manager objects

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the objects you want to delete from this group.
6. Click **Delete**.
7. Confirm to delete the Communication Manager objects.

Filtering Communication Manager objects

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **Filter: Enable** in the group list.
6. Filter the Communication Manager objects according to one or multiple columns.
7. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

   Note:

   The table displays only those devices that match the filter criteria.

Changing to classic view

The System Manager Web interface of Communication Manager objects support two types of views: classic and enhanced. Enhanced view is the default setting, where you can execute tasks on the Web interface. In the classic view, the system directs you to Element Cut Through screen for executing the tasks.

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object you want to manage.
3. By default, the system displays the Web page for the Communication Manager object in enhanced view. To change to classic view, click the **Switch to Classic View** link on the upper-right of the interface.
4. To return to the default view, click the **Switch to Enhanced View** link.

Agents

Agents

Use the Agents capability to manage agent login IDs and skill assignments in an Expert Agent Selection (EAS) environment. If skills are added or changed on the media server, agents must log out and then log in again before the changes are effective.

Agents List

Agents List displays all the agents under the Communication Manager you select. You can perform an advanced search on this list using the search criteria. You can also apply filters and sort each column in the Agents List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
LoginID	Displays the identifier for the Logical Agent as entered in the command line.
Agent Name	Displays the 27-character string name of the agent. Any alphanumeric character is valid. Default is blank.
Direct Agent Skill	Specifies the number of the skill used to handle Direct Agent calls.
Call Handling Preference	Displays which call an agent receives next when calls are in queue.
COR	Displays the Class of Restriction associated with the agent.
System	Specifies the name of the Communication Manager associated with the agents.

Adding an agent

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.

2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the New Agent page and click **Commit**.

Related topics:

Agents field descriptions on page 496

Viewing agent data

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Agents List, select the agent whose data you want to view.
6. Click **View**.

Related topics:

Agents field descriptions on page 496

Editing agent data

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Agents List, select the agent whose properties you want to edit.
6. Click **Edit** or **View** > **Edit**.

7. Edit the required fields on the **Edit Agent** page.
8. Click **Commit** to save the changes.

Related topics:

Agents field descriptions on page 496

Deleting agents

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Agents List, select the agents you want to delete.
6. Click **Delete**.
7. Confirm to delete the agents.

Related topics:

Agents field descriptions on page 496

Adding agents in bulk

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Bulk Add Agents**.
6. Complete the **Bulk Add Agents** page and click **Now**.

The **Agent Name Prefix** field displays the common prefix which appears for all the agents you bulk add. You can enter any prefix name of your choice in this field.

Related topics:

Agents field descriptions on page 496

Editing agent data in bulk

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Bulk Edit Agents**.
6. Complete the **Bulk Edit Agents** page and click **Now**.

   The **Agent Name Prefix** field displays the common prefix which appears for all the agents you bulk add. You can enter any prefix name of your choice in this field.

Related topics:

Agents field descriptions on page 496

Agents field descriptions

Field	Description
Agent Name	Specifies the 27-character string name of the agent. Any alphanumeric character is valid. By default, this field is blank.
AAS	Provides the option to use this extension as a port for an Auto Available Split/Skill. By default, this check box is clear. This option is intended for communication server adjunct equipment ports only, not human agents. **Important:** When you enter y in the AAS field, it clears the password and requires execution of

Field	Description
	the **remove agent-loginid** command. To set AAS to n, remove this logical agent, and add it again.
ACW Agent Considered Idle	Provides the option to count After Call Work (ACW) as idle time. The valid entries are **System**, **Yes**, and **No**. Select **Yes** to have agents who are in ACW included in the Most-Idle Agent queue. Select **No** to exclude ACW agents from the queue.
AUDIX	Provides the option to use this extension as a port for AUDIX. By default, this check box is clear. **Note:** Both AAS and AUDIX fields cannot be y.
AUDIX Name for Messaging	You have the following options: • Enter the name of the messaging system used for LWC Reception. • Enter the name of the messaging system that provides coverage for this Agent LoginID. • Leave the field blank. This is the default setting.
Auto Answer	When using EAS, the auto answer setting of the agent applies to the endpoint where the agent logs in. If the auto answer setting for that endpoint is different, the agent setting overrides the endpoint setting. One of the following is a valid entry: • **all**. Immediately sends all ACD and non-ACD calls to the agent. The endpoint is also given a single ring while a non-ACD call is connected. You can use the ringer-off button to prevent the ring when the feature-related system parameter, **Allow Ringer-off with Auto-Answer**, is set to y. • **acd**. Only ACD split /skill calls and direct agent calls go to auto answer. If this field is set to **acd**, non-ACD calls terminated to the agent ring audibly.

Field	Description
	• **none**. All calls terminated to this agent receive an audible ringing. This is the default setting. • **station**. Auto answer for the agent is controlled by the auto answer field on the Endpoint screen.
Aux Work Reason Code Type	Determines how agents enter reason codes when entering AUX work. One of the following is a valid entry: • **system**. Settings assigned on the Feature Related System Parameters screen apply. This is the default setting. • **none**. You do not want an agent to enter a reason code when entering AUX work. • **requested**. You want an agent to enter a reason code when entering AUX mode but do not want to force the agent to do so. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to y. • **forced**. You want to force an agent to enter a reason code when entering AUX mode. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to y.
Call Handling Preference	Determines which call an agent receives next when calls are in queue. When calls are in queue and an agent becomes available, any of the following entries is valid: • **skill-level**. Delivers the oldest, highest priority calls waiting for the highest-level agent skill. • **greatest-need**. Delivers the oldest, highest priority calls waiting for any agent skill. • **percent-allocation**. Delivers a call from the skill that will otherwise deviate most from its administered allocation. Percent-allocation is available only with Avaya Business Advocate software.

Field	Description
	For more information, see *Avaya Business Advocate User Guide*.
COR	Specifies the Class Of Restriction (COR) for the agent. Valid entries range from **0** to **995**. The default entry is **1**.
Coverage Path	Specifies the coverage path number used by calls to the LoginID. A valid entry is a path number from **1** to **999**, time of day table **t1** to **t999**, or blank by default. Coverage path is used when the agent is logged out, busy, or does not answer calls.
Direct Agent Calls First (not shown)	Provides the option to direct agent calls to override the percent-allocation call selection method and be delivered before other ACD calls. Clear the check box if you want to treat direct agent calls as other ACD calls. This field replaces the Service Objective field when percent-allocation is entered in the Call Handling Preference field. For more information, see *Avaya Business Advocate User Guide*.
Direct Agent Skill	Specifies the number of the skill used to handle Direct Agent calls. A valid entry can range from **1** to **2000**, or blank. The default setting is blank.
Forced Agent Logout Time	Enables the Forced Agent Logout by Clock Time feature by administering a time of day to automatically log out agents using an hour and minute field. A valid entry for the hour field ranges from **01** to **23**. A valid entry for the minute field is **00**, **15**, **30**, or **45**. The default is blank (not administered). Examples are: 15:00, 18:15, 20:30, 23:45.
Local Call Preference	Provides the option to administer Local Preference Distribution to handle agent-surplus conditions, call-surplus conditions, or both. Use this field to administer call-surplus conditions. To set up an algorithm for agent-surplus conditions, set the Local Agent Preference field on the Hunt Group screen. You can select this check box only if the Call Center Release field is set to 3.0 or later and the Multiple Locations customer option is active.

Field	Description
Login ID	Displays the identifier for the Logical Agent as entered in the command line. This is a display-only field.
LoginID for ISDN/SIP Display	Use to include the **Agent LoginID CPN and Name** field in ISDN and SIP messaging over network facilities. By default, the check box is clear, indicating that the physical endpoint extension CPN and Name is sent. If you set the **Send Name** to n or r (restricted) on the ISDN Trunk Group screen, the calling party name and number is sent.
Logout Reason Code Type	Determines how agents enter reason codes. One of the following is a valid entry: • **System**. Settings assigned on the Feature Related System Parameters screen apply. This is the default entry. • **Requested**. You want an agent to enter a reason code when logging out but do not want to force the agent to do this. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to y. • **Forced**. You want to force an agent to enter a reason code when logging out. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to y. • **None**. You do not want an agent to enter a reason code when logging out.
LWC Reception	Indicates whether the terminal can receive Leave Word Calling (LWC) messages. One of the following is a valid entry:: • **audix** • **msa-spe**. This is the default entry. • **none**

Field	Description
Maximum time agent in ACW before logout (Sec)	Sets the maximum time the agent can be in ACW on a per agent basis. One of the following is a valid entry:: • **system**. This is the default entry. Settings assigned on the Feature Related System Parameters screen apply. • **none**. ACW timeout does not apply to this agent. • **30-9999 sec**. Indicates a specific timeout period. This setting will take precedence over the system setting for maximum time in ACW.
Percent Allocation	Specifies the percentage for each of the agent skills if the call handling preference is percent-allocation. a valid entry is a number from **1** to **100** for each skill. Entries for all the agent skills together must add up to 100%. Do not use target allocations for reserve skills. Percent Allocation is available as part of the Avaya Business Advocate software.
Password	Specifies the password the agent must enter upon login. Displayed only if both the AAS and AUDIX check boxes are clear. A valid entry is a digit ranging from **0** through **9**. Enter the minimum number of digits in this field specified by the Minimum Agent-LoginID Password Length field on the Feature-Related System Parameters screen. By default, this field is blank.
Confirm Password	Confirms the password the agent entered in the Password field during login. Displayed only if both the AAS and the AUDIX check boxes are clear. By default, this field is blank. **Note:** Values entered in this field are not echoed to the screen.
Port Extension	Specifies the assigned extension for the AAS or AUDIX port. The values are displayed only if either the AAS or AUDIX check box is selected. This extension cannot be a VDN or an Agent LoginID. By default, this field is blank.

Field	Description
Reserve Level	Specifies the reserve level to be assigned to the agent for the skill with the Business Advocate Service Level Supervisor feature or the type of interruption with the Interruptible AUX Work feature. You can assign a reserve level of 1 or 2 or an interruptible level of a, m, n, or blank for no reserve or interruptible level, where, • a is auto-in-interrupt • m is manual-in-interrupt • n is notify-interrupt Changes to this field take effect the next time the agent logs in. Values of 1 and 2 are allowed only if Business Advocate is enabled. A skill level cannot be assigned with a reserve level setting. Reserve level set to 1 or 2 defines the EWT threshold level for the agent to be added to the assigned skill as a reserve agent. When the EWT for this skill reaches the corresponding threshold set on the Hunt Group screen, this skill gets this skill gets automatically added to the logged in skills of the agents. Agents are delivered calls from this skill until the skill EWT drops below the assigned overload threshold. Use the Interruptible Aux functionality to help meet service level targets by requesting agents who are on break to become available when the service level target is not being met. For more information on Service Level Supervisor, see *Avaya Business Advocate User Guide*.
Service Objective	Provides the option to administer Service Objective. Service Objective is administered on the Hunt Group screen and the agent LoginID screen. This field is displayed only when Call Handling Preference is set to greatest-need or skill-level. The communication server selects calls for agents according to the ratio of Predicted Wait Time (PWT) or Current Wait Time (CWT) and the administered service objective for the skill. Service Objective is part of the Avaya Business Advocate software.

Field	Description
Skill Number	Specifies the Skill Hunt Groups that an agent handles. The same skill cannot be entered twice. You have the following options: • If EAS-PHD is not optioned, enter up to four skills. • If EAS-PHD is optioned, enter up to 20 or 60 skills depending on the platform. **Important:** Assigning a large number of skills to agents can potentially impact system performance. Review system designs with the ATAC when a significant number of agents have more than 20 skills per agent.
Skill Level	Specifies a skill level for each of an agent assigned skills. If you specify the EAS-PHD option, 16 priority levels are available. If you do not specify this option, two priority levels are available.
Tenant Number	Specifies the tenant partition number. A valid entry ranges from **1** to **100**. The default is entry is **1**. **Note:** Values entered in this field are not echoed to the screen.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.
Clear	Clears all entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Announcements

What is an announcement?

An announcement is a recorded message a caller hears while the call is in a queue. An announcement is often used in conjunction with music. Announcements are recorded on special circuit packs (TN750, TN750B,TN750C, or TN2501AP) on your Communication Manager system.

The three types of announcements are:

- delay announcement — explains the reason for the delay and encourages the caller to wait
- forced announcement — explains an emergency or service problem. Use when you anticipate a large number of calls about a specific issue
- information announcement — gives the caller instructions on how to proceed, information about the number called, or information that the caller wants

Announcements are most effective when they are:

- short, courteous, and to-the-point
- spaced close together when a caller on hold hears silence
- spaced farther apart when music or ringing is played on hold
- played for calls waiting in queue

Music on Hold is a package of professionally-recorded music available from Avaya.

Announcement List

Announcement List displays the property of an announcement. To view the announcement list, on the **Elements** menu, navigate to **Communication Manager** > **Call Center** > **Announcements**.

Name	Description
Name	Specifies the file name of the audio file. The alphanumeric file name can contain up to 27 characters.
Extension	Specifies the valid extension number for the announcement. Extension numbers might not include punctuation.
Group/Board	Indicates whether the announcement's audio file exists on the VAL board. Type the group

Name	Description
	number in the format gggV9 for media gateway vVAL, where ggg is the gateway number of the media gateway (up to 250).
Type	Specifies the type of the announcement. Possible values include: • **Integ-mus**. Integrated music type • **Integ-rep**. Integrated repeating type • **Integrated**. Stored internally on a special integrated announcement circuit pack. Use this for general announcements and VDN of Origin Announcements.
Protected	Use this field to set the protection mode for an integrated announcement. When you set this field to **y**, the recording is protected and cannot be deleted or changed through a telephone session or FTP. When you set this field to **n**, you can change or delete the recording if you have the corresponding console permissions.
Rate	If the VAL board is administered on the circuit packs form, then the system automatically displays 64 (64Kbps) in the **Rate** field.
COR	The Class of Restriction associated with this announcement.
TN	Specifies the tenant partition number of the announcement. A valid entry ranges from 1 to 100.
Queue	Specifies the announcement queuing or barge-in. Possible values include: • **no**. This is the default value. Indicates that the announcement does not play if a port is not available. • **yes**. Indicates that the request queues when all ports on the circuit pack are busy. The announcement plays when a port becomes available. This setting is used in most call center applications. • **bargain**. Indicates that you can connect callers to the announcement at any time while it is playing. With **n** or **y**, the caller is always connected to the beginning of the announcement.

Name	Description
Size	Specifies the size of the audio files in kilobytes.
Timestamp	Specifies the date and time the audio file was created or modified. This changes each time the audio file is put on the VAL board using FTP.
System	Specifies the name of the Communication Manager associated with the announcement.

Adding an announcement

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select **New**.
6. Complete the **Add Announcement** page and click **Commit**.

Related topics:

Announcements field descriptions on page 513

Editing an announcement

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the announcement you want to edit from the Announcement List.
6. Click **Edit** or **View** > **Edit**.

7. Edit the required fields on the **Edit Announcement** page.
8. Click **Commit** to save the changes.

Related topics:

Announcements field descriptions on page 513

Viewing an announcement

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the announcement you want to view.
6. Click **View**.
   You can view the properties of the announcement in the **View Announcements** page.

Related topics:

Announcements field descriptions on page 513

Deleting an announcement

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the announcement you want to delete from the Announcement List.
6. Click **Delete**.
7. Confirm to delete the announcements.

Saving an announcement

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the announcement you want to save from the Announcement List.
6. Click **More Actions** > **Save**.
   This action internally edits and updates the announcements in the Communication Manager.

Related topics:

Announcements field descriptions on page 513

Backing up announcements

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the announcements you want to backup.
6. Click **More Actions** > **Backup** to back up your announcements.

Related topics:

Announcements field descriptions on page 513

Backing up all announcements

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Backup All** to back up all the announcements.

Downloading announcements

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Download**.
6. Select the files you want to download from the Backedup Announcements list.
7. Click **Download** to download the backed up announcements.

Related topics:

Announcements field descriptions on page 513

Restoring announcements

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.

4. Click **Show List**.
5. Click **More Actions** > **Restore**.
6. Select a Communication Manager from the Communication Manager list.
7. Select the options from the Restore Options section.
8. If you want to restore from client, select the **Restore from Client** check box.
9. Select the announcements you want to restore from the Backedup Announcement List.
10. Click **Restore** to restore your announcement and announcement property files from your application to a VAL/Virtual VAL board you select.

Related topics:

Announcements field descriptions on page 513

Restoring all announcements

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Restore All**.

Moving an announcement

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Move**.
6. Select the destination where you want to move the announcement.

7. Click **Now** to move the announcement from one VAL board to another within the same voice system.

Related topics:

Announcements field descriptions on page 513

Broadcasting announcements

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the announcements you want to broadcast from the Announcement list.
6. Click **More Actions** > **Broadcast**.
7. Select the destination VAL source.
8. Click **Now** to broadcast the announcement files to various VAL boards on a voice system.

Related topics:

Announcements field descriptions on page 513

Using File Transfer Settings

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select an announcement from the Announcement List.
6. Click **More Actions** > **File Transfer Settings**.
7. Select a VAL board from the VAL Board and Media Gateway list.

8. Click **Done**.

Related topics:

Announcements field descriptions on page 513

Using List Usage Extension

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select an announcement from the Announcement List.
6. Click **More Actions** > **List Usage Extension**.
   You can view the details of the announcement through the List Usage for Extension list.
7. Click **Done**.

Related topics:

Announcements field descriptions on page 513

Filtering the Announcements list

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Click **Filter: Enable** in the Announcement list.
4. Filter the list according to one or multiple columns.
5. Click **Apply**.
   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

Note:

The table displays only those options that match the filter criteria.

Using Advanced Search

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **Advanced Search** in Announcement List.
6. In the Criteria section, do the following:
   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter the search value in the third field.

   If you want to add a search condition, click the plus sign (**+**) and repeat the substeps listed in Step 5.

   If you want to delete a search condition, click the minus sign (**-**) . This button is available if there is more than one search condition.
7. Click **Search**.

Announcements field descriptions

Name	Description
Name	Specifies the filename of the audio file. The filename can be up to 27 characters and must be alphanumeric.
Extension	Valid extension number for the announcement. Extension numbers may not include punctuation.
Group/Board	This field indicates whether the announcement's audio file exists on the VAL board. Type the group number in the format

Name	Description
	gggV9 for media gateway vVAL, where *ggg* is the gateway number of the media gateway (up to 250).
Type	Specifies the type of the announcement. Possible values include: • **Integ-mus**. Integrated music type • **Integ-rep**. Integrated repeating type • **Integrated**. Stored internally on a special integrated announcement circuit pack. Use this for general announcements and VDN of Origin Announcements.
Protected	Use this field to set the protection mode for an integrated announcement. When you set this field to **y**, the recording is protected and cannot be deleted or changed through a telephone session or FTP. When you set this field to **n**, you can change or delete the recording if you have the corresponding console permissions.
Rate	The recording rate speed for announcements. If the VAL board is administered on the circuit packs form, then 64 (64Kbps) automatically appears in this field.
COR	The Class of Restriction associated with this announcement.
TN	Specifies the tenant partition number of the announcement. Valid entries include 1 to 100.
Queue	Specifies the announcement queuing or barge-in. Possible values include: • **no** (default)- indicates that the announcement does not play if a port is not available. • **yes** indicates that the request queues when all ports on the circuit pack are busy. The announcement plays when a port becomes available. This setting is used in most call center applications. • **bargain** indicates that you can connect callers to the announcement at any time while it is playing. With n or y, the caller is

Name	Description
	always connected to the beginning of the announcement.
Size	The size of the audio file in kilobytes.
Timestamp	The date and time the audio file was created or modified. This changes each time the audio file is uploaded.
System	Specifies the name of the Communication Manager associated with the announcement.

Audio File Information

Name	Description
Use Unused Wave File	Select the check box to use an audio file that has not been used yet.
Upload Audio File	You can upload an audio file through this option by browsing to the file you want to upload.

More Actions in Audio Groups field description

Name	Description
File Name	Specifies the filename of the audio file. The filename can be up to 27 characters and must be alphanumeric.
File Size	The size of the audio file in kilobytes.
Backup Announcement Properties	Backs up the announcement property
Backup Wave Files	Backs up the WAVE files only
Backup Both (Announcement Properties with associated wave file)	Backs up both the announcement property and the WAVE file for the announcement.
Restore Announcement Properties	Restores only your announcement properties
Restore Wave Files	Restores only the wave files present for the announcement.
Restore Both (Announcement Properties with associated wave file)	Restores both the announcement property and the wave file for the announcement.
VAL Board	Specifies the group number of the VAL board. Type the group number in the format gggV9 for media gateway vVAL, where *ggg*

Name	Description
	is the gateway number of the media gateway (up to 250). Type the board format as: cabinet(01-64): carrier(A-E): slot(01-20). For example, 03A10.
Type	Specifies whether the Announcement is a VAL Announcement or a Media Gateway (MG) Announcement.
Transfer Mode	Type of transfer used to backup or restore or upload audio files. Possible values are FTP, SFTP, and, SCP.
Used By	Specifies the object in which the extension is used. For example Endpoint, Announcement etc.
Object info	Specifies the details of the object.
Used as	Specifies how the extension is used in the object.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.
Clear	Clears all the entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Download	Downloads the audio files or announcement files.
Now	Performs the action you initiate real time.
Restore	Restores your announcements on the voice system you select.

Audio Groups

What is an audio group?

An audio group is a logical container that holds VAL sources. An audio group can hold several VAL Sources which can be VAL Boards or media gateways.

Adding an audio group

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Audio Group**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Audio Groups** page and click **Commit**.

Related topics:

Audio Groups field descriptions on page 519

Editing an audio group

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Audio Group**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the audio group you want to edit.
6. Click **Edit** or **View** > **Edit**.

7. Edit the required fields and click **Commit** to save the changes.

Related topics:

Audio Groups field descriptions on page 519

Viewing an audio group

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Call Center** > **Audio Group** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the audio group you want to view.
6. Click **View** to view the properties of the audio group.

Related topics:

Audio Groups field descriptions on page 519

Deleting an audio group

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Audio Group**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the audio groups you want to delete from the Audio Groups List.
6. Click **Delete**.
7. Confirm to delete the audio groups.

Using More Actions

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Audio Group**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select an audio group from the Audio Groups List.
6. Click **More Actions**.
7. Do one of the following:
   - Click **Backup** to back up the audio groups you selected on a voice system.
   - Click **Download** to download the audio groups you selected.
   - Click **Restore** to restore the audio groups on a voice system you select.

Related topics:

Audio Groups field descriptions on page 519

Audio Groups field descriptions

Name	Description
System	Specifies the device type. In this case, the Communication Manager you choose.
Group Number	Specifies the audio group number.
Group Name	Specifies the name of the audio group.

Members List

Name	Description
Group/Board	This field indicates whether the announcement's audio file exists on the VAL board. Type the group number in the format gggV9 for media gateway vVAL, where *ggg* is the gateway number of the media gateway (up to 250).

Name	Description
Is Member	Specifies whether the VAL board or the Media gateway shown is a member in the audio group.

Note:

You can filter the Members list according to one or multiple columns using the **Filter: Enable** option in the list.

More Actions in Announcements- field descriptions

Name	Description
CM	Specifies the Communication Manager you have chosen.
Backup Announcement Properties	Backs up the announcement property.
Backup Wave Files	Backs up the waves files only.
Backup Both (Announcement Properties with associated wave file)	Backs up both the announcement property and the wave file for the announcement.
File Name	Name of the audio group.
File Size	Specifies the size of the audio file in kilobytes.
Restore Announcement Properties	Restores only your announcement properties.
Restore Wave Files	Restores only the wave files present for the announcement.
Restore Both (Announcement properties with Associated wave file)	Restores both the announcement property and the wave file for the announcement.
Restore from client	Select this checkbox if you want to restore from the client machine.

Button	Description
Commit	Performs the action you initiate.
Schedule	Performs the action at the specified time.
Reset	Clears the action and resets the fields.
Clear	Clears all the entries.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.

Button	Description
Restore	Restores your announcements on the voice system you select.
Backup	Backs up the audio files that you select.
Download	Downloads the audio files or announcement files.
Now	Performs the action you initiate real time.

Vector Directory Number

Vector Directory Number

The Vector Directory Number capability defines the vector directory numbers (VDN) for the Call Vectoring feature. A VDN is an extension number used to access a call vector. Each VDN is mapped to one call vector. VDNs are software extension numbers that is, not assigned to physical equipment. A VDN is accessed through direct dial local telephone company central office trunks mapped to the VDN (incoming destination or night service extension), DID trunks, and LDN calls. The VDN can be Night Destination for LDN.

Vector Directory Number List

Vector Directory Number List displays all the Vector Directory Number (VDN) details under the Communication Manager you select. You can view the usage list of the extension you select in this list. You can also apply filters and sort each of the columns in the Vector Directory Number List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Extension	Displays the extension number of the Vector Directory Number.
Name	Displays the name associated with the Vector Directory Number.
Destination	Indicates whether the calls are routed using a Vector Number or Policy Routing Table.
Allow VDN Override	Indicates whether the routed-to Vector Directory Number is changed to active VDN for the call.

Name	Description
COR	Displays the Class Of Restriction (COR) of the Vector Directory Number consisting of a one or two-digit number.
TN	Displays the tenant partition number.
System	Specifies the name of the Communication Manager associated with the vector directory number.

Adding Vector Directory Number

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Vector Directory Number (VDN)** page and click **Commit**.

Viewing Vector Directory Number

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select the vector directory number you want to view.
6. Click **View**.

Editing Vector Directory Number

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select the vector directory number you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Directory Number (VDN)** page.
8. Click **Commit** to save the changes.

Deleting Vector Directory Number

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select the vector directory number you want to delete.
6. Click **Delete**.
7. Confirm to delete the vector directory number.

List Usage Extension in Vector Directory Number

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.

2. Click **Call Center** > **Vector Directory Number** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select a vector directory number.
6. Click **More Actions** > **List Usage Extension**.
7. Click **Done**.

   You can view the details of the vector directory number in the List Usage for Extension list.

Vector Routing Table

Vector Routing Table

Use Vector Routing Table to store ANI or digits that you refer to in the **goto** vector steps. This capability is available only if the **Vectoring (G3V4 Enhanced)** field on the System-Parameters Customer-Options screen is set to **y**.

Vector Routing Table List

Vector Routing Table List displays all the Vector Routing Tables under the Communication Manager you select. You can also apply filters and sort each of the columns in the Vector Routing Table List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Number	Displays the table number you entered on the command line.
Name	Displays the 1 to 15-character alphanumeric table name. By default, this field is blank.
Sort	Enables you to sort the digit fields.
Number Of Entries	Displays the number of entries in the dialing list.
System	Specifies the name of the Communication Manager associated with the Vector Routing Table.

Adding Vector Routing Table

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Routing Table**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Vector Routing Table** page and click **Commit**.

Related topics:

Vector Routing Table field descriptions on page 526

Viewing Vector Routing Table

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Routing Table**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Routing Table List, select the vector routing table you want to view.
6. Click **View**.

Related topics:

Vector Routing Table field descriptions on page 526

Editing Vector Routing Table

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Routing Table**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Routing Table List, select the vector routing table you want to edit.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields on the **Edit Vector Routing Table** page.
8. Click **Commit** to save the changes.

Related topics:

Vector Routing Table field descriptions on page 526

Deleting Vector Routing Table

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Routing Table**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Routing Table List, select the vector routing tables you want to delete.
6. Click **Delete**.
7. Confirm to delete the selected vector routing tables.

Related topics:

Vector Routing Table field descriptions on page 526

Vector Routing Table field descriptions

Field	Description
Name	Specifies the 1 to 15-character alphanumeric table name or blank. By default, this field is blank.
Number	Specifies the table number you entered on the command line. This is a display-only field.
Digit String	Entries in this field can include the plus sign (+) and question mark (?) wildcard. The plus sign (+) represents a group of digits. The question mark (?) represents a single digit. By default, this field is blank. The field is limited to 16 characters and these characters are restricted as follows: • You can enter only a plus sign (+), a question mark (?), or the numbers 0 through 9. No other entries are valid. • You can enter a plus sign (+) as either the first or last character in the number field. However, you cannot use this character as the sixteenth character of the number field. • You can use unlimited question marks (?) anywhere in the number field. • You should not embed blanks in the number field. • You can leave the field entirely blank. If you do, the communication server will store the entry as a null value.
Sort	Provides the option to sort the digit fields. By default, this check box is clear. If you do not to sort the numbers, they will remain in the order that you entered them. If you sort the number fields, they will be sorted as described below. Remember that leading zeros are significant. That means that 02 will sort ahead of a 2 followed by a space. • Any plus signs (+) will sort first. • Any question marks (?) will sort second. • All numbers (0-9) will sort last.
Route Number	Displays the static route numbers that are available in the selected vector routing table.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.
Clear	Clears all entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate in real time.

Coverage Path

Coverage Path

Use Coverage Path to implement call coverage paths by providing the means to specify the call coverage criteria, the points in the coverage path used to redirect calls, and the number of times a principal telephone rings before the call redirects to coverage.

Coverage Path List

Coverage Path List displays all the coverage path details under the Communication Manager you select. You can also apply filters and sort each column in the Coverage Path List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Coverage Path Number	Displays the coverage path that is being administered.
Next Path Number	Displays the number of the next coverage path in a coverage path chain.
Hunt after Coverage	Indicates whether the coverage treatment is continued or terminated.

Name	Description
Number of Rings	Displays the number of times a telephone rings before the system redirects the call to the first point in the coverage path.
System	Specifies the name of the Communication Manager associated with the coverage path.

Adding Coverage Path

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Path**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Coverage Path** page and click **Commit**.

Related topics:

Coverage Path on page 531

Viewing a Coverage Path

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Path**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Path List, select the coverage path you want to view.
6. Click **View**.

Related topics:

Coverage Path on page 531

Editing a Coverage Path

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Path**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Path List, select the coverage path you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Coverage Path** page.
8. Click **Commit** to save the changes.

Related topics:

Coverage Path on page 531

Deleting a Coverage Path

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Path**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Path List, select the coverage path you want to delete.
6. Click **Delete**.
7. Confirm to delete the coverage path.

Related topics:

Coverage Path on page 531

Coverage Path

Implements Call Coverage Paths by providing the means to specify the call coverage criteria, the points in the coverage path used to redirect calls, and the number of times a principal's telephone rings before the call redirects to coverage.

Coverage Path Number

The coverage path being administered.

Cvg Enabled for VDN Route-To Party

Enables or disables the route-to party coverage path after a covered call hits a VDN vector route-to step. By default, the value is n.

Holiday Coverage

Holiday coverage must be set separately for both inside and outside calls.

Valid Entry	Usage
y	Sends the call to an announcement.
n	Sends the call to the next point in the coverage path.

Holiday Table

Available only when **Holiday Coverage** is set to y for inside or outside calls.

The number of the holiday table used for holiday coverage.

Hunt After Coverage

Valid Entry	Usage
y	Coverage treatment continues by searching for an available station in a hunt chain that begins with the hunt-to-station assigned to the station of the last coverage point.
n	Coverage treatment is terminated. The call is left at the last available location, the principal or coverage point.

Linkage

One or two additional coverage paths in the coverage path chain.

Next Path Number

Valid Entry	Usage
1 to 9999	The number of the next coverage path in a coverage path chain. If the coverage criteria of the current coverage path is dissatisfied, the system checks in this chain until it finds a coverage path with redirection criteria that matches the call status. If the chain is exhausted before the system finds a match, the call stays out of coverage.
blank	The only path for the principal.

COVERAGE CRITERIA

COVERAGE CRITERIA

Assigns coverage criteria. When met, it redirects the call to coverage.

Valid Entry	Usage
Active	Calls redirect if at least one call appearance is busy.
Busy	Calls redirect if all call appearances that accept incoming calls are busy.
Don't Answer	Calls redirect when the specified number of rings has been exceeded.
All	Calls redirect immediately to coverage. Overrides any other criteria administered for this field.
DND/SAC/Go to Cover	A calling user, when calling to another internal extension, can redirect a call immediately to coverage by pressing the **Go to Cover** button. A principal can temporarily direct all incoming calls to coverage, regardless of the other assigned coverage criteria by pressing the **Send All Calls** or **Do Not Disturb** button. **Send All Calls** also allows covering users to temporarily remove their telephones from the coverage path. Must be assigned before a user can activate Do Not Disturb (Hospitality Services), Send All Calls (SAC), or Go to Cover features.
Logged off/PSA/TTI	The system displays this field appears only when the **Criteria for Logged Off/PSA/TTI Stations** field is set to y. Calls redirect to coverage after the number of rings exceeds the number specified in the **Number of Rings** field. By default, the value of the **Criteria for Logged Off/PSA/TTI Stations** field is y. The system displays the associated **Number of Rings** field only when the **Logged off/PSA/TTI** field is set to y.

Number of Rings

Valid Entry	Usage
1 to 99	The number of times a telephone rings before the system redirects the call to the first point in the coverage path. By default, the value is 2.

COVERAGE POINTS

Point1, Point2, Point3, Point4, Point5, Point6

The alternate destinations that comprise a coverage path. Coverage points must be assigned sequentially without steps beginning with Point 1. Each path can have up to six coverage points.

Subsequent coverage points should be unlisted if calls are redirected to:

- Message Center, a special Uniform Call Distribution hunt group
- Voice messaging
- The attendant

These calls normally queue and never redirect to another coverage point. Calls to hunt group queue if possible. Calls redirect from a hunt group only if all hunt group members are busy and either the queue is full, or is nonexistent.

If the Coverage of Calls Redirected Off-Net feature is not supported, a remote coverage point functions as the last point in the coverage path because the system can no longer control calls once they redirect off-net. However, if the Coverage of Calls Redirected Off-Net feature is enabled, calls redirected off-net can be monitored by the system and brought back for call coverage processing.

Valid Entry	Usage
extension	Redirects the call to an internal extension or announcement. **Note:** When entering a shortened extension of a Multi-Location Dial Plan in a field designed for announcement extensions, certain administration and validation of announcement extensions are not performed. Therefore, the system does not display resultant warnings or submittal denials. Extra care should be taken to administer the correct type of announcement for the application if assigning shortened extensions.
attd	Redirects the call to the attendant or attendant group. If the system has Centralized Attendant Service (CAS), the call goes to the CAS attendant.
h1 to h999	Redirects the call to the corresponding hunt-group, for example, `h32` routes to hunt group 32.
c1 to c750 c1 to c1000 (S8300D/duplex Media Servers)	Redirects the call to the corresponding coverage answer group, for example, `c20` routes to call coverage answer group 20.
r1 to r999 r1 to r1000 S8300D/duplex (Media Servers)	Redirects the call to the corresponding remote coverage point number, for example, `r27` routes to remote coverage point 27.
v + extension	Redirects the call to the corresponding Vector Directory Number (VDN) extension, for example, `v12345` routes to the VDN associated with extension 12345. **Note:** A VDN can be used only as the last administered point in a coverage plan.
y + extension	Redirects the call to an internal extension, announcement, or the corresponding Vector Directory Number (VDN) extension as per the current date and time set in Holiday Table.

Rng

Valid Entry	Usage
1 to 99 blank	The number of rings at this coverage point before the system redirects the call to the next point in the coverage path.

Terminate to Coverage Pts. with Bridged Appearances

Valid Entry	Usage
y	If activated, a call can alert as both a bridged call and a redirected call.
n	The call skips the coverage point if it has already alerted as a bridged call.

Coverage Time-of-day

Coverage Time-of-day

Use Coverage Time-of-day to administer up to five different coverage paths associated with five different time ranges, for each day of the week. Only one coverage path can be in effect at a given time.

Coverage Time-of-day List

Coverage Time-of-day List displays all the coverage time-of-day details under the Communication Manager you select. You can also apply filters and sort each column in the Coverage Time-of-day List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Number	Displays the Coverage Time-of-day table number.
System	Specifies the name of the Communication Manager associated with the vector directory number.

Adding Coverage Time-of-day

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Coverage Time-of-day Data** page and click **Commit**.

Related topics:

Time of Day Coverage Table on page 536

Viewing Coverage Time-of-day

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Time-of-day List, select the coverage time-of-day you want to view.
6. Click **View**.

Related topics:

Time of Day Coverage Table on page 536

Editing Coverage Time-of-day

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Time-of-day**.

3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Time-of-day List, select the coverage time-of-day you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Coverage Time-of-day Data** page.
8. Click **Commit** to save the changes.

Related topics:

Time of Day Coverage Table on page 536

Deleting Coverage Time-of-day

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Time-of-day List, select the coverage time-of-day you want to delete.
6. Click **Delete**.
7. Confirm to delete the coverage time-of-day.

Related topics:

Time of Day Coverage Table on page 536

Time of Day Coverage Table

This screen allows administration of up to five different coverage paths, associated with five different time ranges, for each day of the week. Only one coverage path can be in effect at any one time.

Act Time

Valid Entry	Usage
00:01– 23:59	Specifies the activation time of the associated coverage path. Information must be entered in 24-hour time format. If there are time gaps in the table, there will be no coverage path in effect during those periods. The first activation time for a day is set to 00:00 and cannot be changed. Activation times for a day must be in ascending order from left to right.

CVG Path

Valid Entry	Usage
1 to 9999 blank	The coverage path number.

Time of Day Coverage Table

Displays the Time of Day Coverage Table number.

Endpoints

Endpoint management

In System Manager, you can create and manage endpoints using the **Manage Endpoints** option. You can also manage other endpoint related objects such as, Alias Endpoints, Intra Switch CDR, Off PBX Endpoint Mappings, Site Data, and Xmobile Configuration. Additionally, using the **Manage Endpoints** option you can also view, edit, and delete endpoints and other endpoint related objects. System Manager provides support for the following set types:

Category	Set Type
IP/SIP Set types	9610SIP/9620SIP/9630SIP/9640SIP/ 9650SIP 9608SIP/9621SIP/9641SIP/9611SIP 9610/9620/9630/9640/9650 9608/9611/9621/9641 1603/1608/1616CC 9600SIP 4620SIP 9608SIPCC/9611SIPCC/9621SIPCC/ 9641SIPCC 4610/4620/4621/4622/4625/4630 4602+ 4612CL H.323

DCP Set types	2402/2410/2420 9404/9408 6402/6402D/6408/6408+/6408D/6408D+/ 6416D+/6424D+ 8403B/8405B/8405B+/8405D/8405D+/ 8410B/8410D/8411B/8411D/8434D 1408 1416
Analog Set types	2500
BRI Set types	WCBRI
X-Mobile endpoints	XMOBILE. Configured as ISDN DECT, IP DECT, PHS, or EC500 type endpoints

Note:

The set types supported varies based on the Communication Manager versions managed.

Adding an endpoint

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Select the template based on the set type you want to add.
   The system displays all the sections on the **Add Endpoint** page.
7. To add the endpoint, complete the information on the Add Endpoint page and click **Commit**.

   Before adding an endpoint, complete the mandatory fields that are marked with a red asterisk (*). in the sections: **General options**, **Feature Options**, **Site Data**, **Data Module/Analog Adjunct**, **Abbreviated Call Dialing**, **Enhanced Call Fwd**, and **Button Assignment**.

   Note:

   To add an endpoint with a non-supported set type, add the endpoint using Element Cut Through. For alias endpoints, you can choose the corresponding Alias set type from the **Template** field. System Manager automatically creates a template for the Alias set types based on the “aliased-to” set type. Alias endpoint templates have names beginning with “Alias”. Before the system displays the

Alias endpoint type template in the drop-down menu, you must create an alias set type on the managed Communication Manager. You can then use the template to add an endpoint.

Related topics:

Endpoint / Template field descriptions on page 550

Using Native Name

Before you begin

- To enter the native name:
  - you need the Input Method Editor (IME) application.
  - You must manually enable IME.

Note:

If IME is not enabled, the keyboard input remains in the default language.

,

About this task

Using the IME application you can enter characters in multiple languages such as Japanese, Korean, Russian, Arabic, and Chinese without requiring a special keyboard.

The IME icon appears in the Windows system tray and indicates the language you are currently using. For example, if you are using English, the IME icon in the system tray displays **EN**. If you are using French, the IME icon in the system tray displays **FR**.

Procedure

1. Click the IME icon in the Windows system tray.

   The system displays a menu with the languages installed on your PC.
2. Select the language you want to use.
3. Type the native name in .

Editing an endpoint

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.

2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to edit from the Endpoint List.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields in the **Edit Endpoint** page.
8. Click **Commit** to save the changes.

Related topics:

Endpoint / Template field descriptions on page 550

Duplicating an endpoint

About this task

The Duplicate Endpoint functionality is to support the “duplicate station” command on Communication Manager. Use this functionality to copy information from an existing endpoint and modify it for each new endpoint. For example, you can configure one endpoint as desired for an entire work group. Then, you merely duplicate this endpoint to all the other extensions in the group. Note that only endpoints of the same type can be duplicated. This functionality copies all the feature settings from the selected endpoint to the new endpoints. You can duplicate up to 16 endpoints at one time.

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to duplicate from the Endpoint List and click **Duplicate**.
6. On the Duplicate Endpoint page, complete the required fields.
7. Click **Commit** to duplicate the endpoint or do one of the following:
   - Click **Schedule** to duplicate the endpoint at a specified time.
   - Click **Cancel** to cancel the operation.

Related topics:

Endpoint / Template field descriptions on page 550

Viewing an endpoint

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to view from the Endpoint List.
6. Click **View** to view the attributes of the endpoint you have chosen.

Note:

You cannot edit the fields in the View Endpoint page. To go to the Edit Endpoint page, click **Edit**.

Related topics:

Endpoint / Template field descriptions on page 550

Deleting an endpoint

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to delete from the Endpoint List.
6. Click **Delete**.

   The system displays a confirmation message alerting you to a user associated with the endpoint. The system highlights these user-associated endpoints in yellow color.

Note:

You cannot delete an endpoint associated with a user through endpoint management. You can delete the user associated endpoints only through User Profile Management.

Related topics:

Endpoint / Template field descriptions on page 550

Editing endpoint extensions

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint from the Endpoint List for which you want to edit the extension.
6. Click **More Actions** > **Edit Endpoint Extension**.
7. Complete the **Edit Endpoint Extension** page and click **Commit** to save the new extension.

Note:

You can use the **Edit Endpoint Extension** option to change the endpoint extension. You can also edit the **Message Lamp Ext** and **Emergency Location Ext** fields through **Edit Endpoint Extension**. Use the **Edit** option to modify the other attributes.

Related topics:

Edit Endpoint Extension field descriptions on page 569

Bulk adding endpoints

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.

2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Bulk Add Endpoints**.
6. Complete the **Bulk Add Endpoint** page and click **Commit** to bulk add the endpoints.

   The **Endpoint Name Prefix** field gives the common prefix which appears for all the endpoints you bulk add. You can enter any prefix name of your choice in this field.

   Note:

   In the **Enter Extensions** field, you can enter the extensions that you want to use. You must enter the extensions in a serial order and also check for the availability of an extension before you use it.

Related topics:

Bulk Add Endpoint field descriptions on page 570

Bulk editing endpoints

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to edit in bulk from the Endpoint List.
6. Click **More Actions** > **Bulk Edit Endpoints**.
7. Complete the **Bulk Edit Endpoint** page and click **Commit** to bulk edit the endpoints.

   The **Endpoint Name Prefix** field gives the common prefix that the system displays for all the endpoints you bulk add or edit. You can enter any prefix name of your choice in this field.

Related topics:

Bulk Edit Endpoint field descriptions on page 571

Filtering endpoints

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **Filter: Enable** in the Endpoint List.
6. Filter the endpoints according to one or multiple columns.
7. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

   Note:

   The table displays only those endpoints that match the filter criteria.

Related topics:

Endpoint / Template field descriptions on page 550

Using Advanced Search

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **Advanced Search** in the Endpoint list.
6. In the Criteria section, do the following:
   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter the search value in the third field.

If you want to add a search condition, click the plus sign (**+**) and repeat the sub steps listed in Step 5.

If you want to delete a search condition, click the minus sign (**-**). This button is available if there is more than one search condition.

Related topics:

Endpoint / Template field descriptions on page 550

Changing endpoint parameters globally

Use the Global Endpoint Change capability to bulk edit endpoint properties globally across one or multiple Communication Manager systems.

You can modify the endpoint properties manually or opt to modify the endpoint properties based on a default template. You can select your preferred default template from the **Template Name** drop-down list under the **General Options** tab. After you select your preferred default template, the system overwrites the field values under the different property tabs, such as General Options, Feature Options, and Button Assignment with those in the default template. You can modify the endpoint properties of the default template to meet your requirement. This customization does not impact the default template as the system only applies the changes to the listed extensions.

For example, you can find all the buttons or features with a specific assign and change the parameters for all those buttons or features respectively, locate new buttons without overwrite, and change the set type of many endpoints simultaneously as you move from digital to IP or SIP.

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. On the Endpoints page, select the endpoints from the Endpoints List for which you want to change the parameters.
4. Click **More Actions** > **Global Endpoint Change** .
5. On the Endpoint Changes page, set the error configuration option in **Select Error Configuration**. The options are:
   - **Continue processing other records**: When you select this option, the system skips the erroneous record and continues to process the other records. This is the default setting.
   - **Abort on first error**: When you select this option, the system aborts the importing process on encountering the first error.

6. Perform one of the following:
   - Modify the fields manually under each of the tabs, as required.
   - Under the **General Options** tab, select your preferred default template from the **Template Name** drop-down and update the property fields as required. The system overwrites all the field values with those in the template. This update does not affect the default template as the system only applies the changes to the listed extensions.
7. Click **Commit** to apply the changes to the endpoint parameters, or do one of the following:
   - Click **Schedule** to change the endpoint parameters at a specified time.
   - Click **Cancel** to cancel the operation.

Related topics:

Endpoint / Template field descriptions on page 550

Viewing endpoint status

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. From the Endpoint List, select the endpoints whose status you want to view.
4. Click **Maintenance** > **Status**.

Result

The system displays the status of the selected endpoint on the Element Cut Through screen.

Related topics:

Endpoint / Template field descriptions on page 550
Error codes on page 572

Busy out endpoints

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select the endpoints you want to busy out from the Endpoint List.

   Important:

   This maintenance operation is service affecting.
4. Click **Maintenance** > **Busyout Endpoint**.
5. On the Busyout Endpoint Confirmation page, click **Now** to busy out the endpoints or do one of the following:
   - Click **Schedule** to perform the busy out at a specified time.
   - Click **Cancel** to cancel the busy out.

Result

The system displays the result of the busy out operation on the **Busyout Endpoint Report** page.

Related topics:

Endpoint / Template field descriptions on page 550
Error codes on page 572

Releasing endpoints

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select the endpoints you want to release from the Endpoint List.

   Important:

   This maintenance operation is service affecting.
4. Click **Maintenance** > **Release Endpoint**.
5. On the **Release Endpoint Confirmation** page, click **Now** to release the endpoints or do one of the following:
   - Click **Schedule** to perform the release at a specified time.

- Click **Cancel** to cancel the release.

Result

The system displays the result of the release operation on the **Release Endpoint Report** page.

Related topics:

Endpoint / Template field descriptions on page 550
Error codes on page 572

Testing endpoints

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select the endpoints you want to test from the Endpoint List.

   Important:

   This maintenance operation is service affecting.
4. Click **Maintenance** > **Test Endpoint**.
5. On the Test Endpoint Confirmation page, click **Now** to test the endpoints or do one of the following:
   - Click **Schedule** to test the endpoints at a specified time.
   - Click **Cancel** to cancel the test operation.

Result

The system displays the **Test Endpoint Report** page, where you can view the test result and error code of the endpoint. Click the **Error Code Description** link to view the error details.

Related topics:

Endpoint / Template field descriptions on page 550
Error codes on page 572

Using Clear AMW All

Clear AMW All is one of maintenance operations listed under the **Maintenance** drop-down on the Manage Endpoints page. You can perform this operation on a single or multiple endpoints

from the Endpoint List. In this maintenance operation, for each endpoint, the system runs the following SAT command

```
clear amw all <endpoint>
```

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select the endpoints from the Endpoint List for which you want to use this functionality.
4. Click **Maintenance** > **Clear AMW All**.
5. On the **Clear AMW All Confirmation** page, click **Now** to perform this task immediately, or do one of the following:
   - Click **Schedule** to perform this task at a specified time.
   - Click **Cancel** to cancel this task.

   The system displays a confirmation that the command has been completed and returns you to the Manage Endpoint landing page.

Using Swap Endpoints

About this task

Use this functionality to swap location site data between two endpoints of the same type and the same Communication Manager system. For Analog and DCP endpoint types, this functionality also swaps the physical port information. While swapping the endpoint data, you also have the option to assign new location site data to the endpoints.

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Swap Endpoints**.
6. On the Swap Endpoints page, enter endpoint extension values in the fields **Endpoint 1** and **Endpoint 2**.
7. Click **Show Details**. The system displays the location site data for each endpoint under the respective endpoint tabs.

8. Click **Commit** to swap data between the two endpoints.
9. To assign new values to the endpoints, perform the following:
   a. Click the endpoint tab whose data you want to change.
   b. Select the **Assign data for Endpoint**<*n*> check box.
   c. Enter the required values for the endpoint under **Descriptions**.
   d. Click **Commit**.

Related topics:

Endpoint / Template field descriptions on page 550
Swap Endpoints field descriptions on page 571

Endpoint List

Endpoint List displays all the endpoints under the Communication Managers you select. You can perform an advanced search on the endpoint list using the search criteria. You can also apply filters and sort each of the columns in the Endpoint List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Name	Specifies the name of the endpoint.
Extension	Specifies the extension of the endpoint.
Port	Specifies the port of the endpoint.
Set Type	Specifies the set type of the endpoint.
COS	Specifies the Class Of Service for the endpoint.
COR	Specifies the Class Of Restriction for the endpoint.
User	If an endpoint is associated with a user, the system displays the name of that user in this column.
System	Specifies the Communication Manager of the endpoint.

Add Endpoint Template

Endpoint / Template field descriptions

You can use these fields to perform endpoint / template tasks. This page has the exclusive fields that occur for endpoints and templates apart from the **General options**, **Feature**

Options, **Site Data**, **Data Module/Analog Adjunct**, **Abbreviated Call Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.

Field description for Endpoints

Name	Description
System	Specifies the Communication Manager that the endpoint is assigned to.
Template	Specifies all the templates that correspond to the set type of the endpoint.
Set Type	Specifies the set type or the model number of the endpoint.
Name	Specifies the name associated with an endpoint. The system displays the name you enter on called telephones that have display capabilities. In some messaging applications, such as Communication Manager Messaging, you enter the user name (last name first) and their extension to identify the telephone. The name entered is also used for the integrated directory.

Field description for Templates

Name	Description
Set Type	Specifies the set type or the model of the endpoint template.
Template Name	Specifies the name of the endpoint template. You can enter the name of your choice in this field.

Extension

The extension for this station.

Port

The Auxiliary and Analog ports assigned to the station are as follows.

Valid Entry	Usage
01 to 64	The first and second numbers are the cabinet numbers.
A to E	The third character is the carrier.
01 to 20	The fourth and fifth characters are the slot numbers. G650 has 14 slots.
01 to 32	The sixth and seventh characters are the port numbers.

Valid Entry	Usage
x or X	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension has a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions.
IP	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have an IP set. This is automatically entered for certain IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.
xxxVmpp	Specifies the Branch Gateway. • xxx is the Branch Gateway number, which is in the range 001 to 250. • m is the module number, which is in the range 1 to 9. • pp is the port number, which is in the range 01 to 32.
Analog Trunk port	Analog trunk port is available with: • MM711 and MM714 media modules • TN747 and TN797 circuit packs

General Options

This section lets you set the general fields for a station.

COS

The Class of Service (COS) number used to select allowed features.

Continue on Error

When the system encounters an error, provides an option to continue or abort the implementation of parameter changes.

COR

Class of Restriction (COR) number with the required restriction.

Coverage Path 1 or Coverage Path 2

The coverage-path number or time-of-day table number assigned to the station.

Note:

If Modified Misoperation is active, a Coverage Path must be assigned to all stations on Communication Manager.

TN

Valid Entry	Usage
1 to 100	The Tenant Partition number.

Security Code

The security code required by users for specific system features and functions are as follows:

- Extended User Administration of Redirected Calls
- Personal Station Access
- Redirection of Calls Coverage Off-Net
- Leave Word Calling
- Extended Call Forwarding
- Station Lock
- Voice Message Retrieval
- Terminal Self-Administration
- Enterprise Mobility User
- Extension to Cellular
- Call Forwarding
- Posted Messages
- Security Violation Notification
- Demand Printing

The required security code length is administered system wide.

Emergency Location Ext

The Emergency Location Extension for this station. This extension identifies the street address or nearby location when an emergency call is made. Defaults to the telephone's extension. Accepts up to thirteen digits.

Note:

On the ARS Digit Analysis Table in Communication Manager, 911 must be administered to be call type emer or alrt for the E911 Emergency feature to work properly.

Message Lamp Ext

The extension of the station tracked with the message waiting lamp.

Lock Messages

Controls access to voice messages by other users.

Valid Entry	Usage
y	Restricts other users from reading or canceling the voice messages, or retrieving messages using Voice Message Retrieval.
n	Allows other users to read, cancel, or retrieve messages.

Feature Options

This section lets you set features unique to a particular voice terminal type.

Location

This field appears only when the **Multiple Locations** field on the system parameters customer options screen is set to y and the **Type** field is set to H.323 or SIP station types.

Valid entry	Usage
1 to 250	(Depending on your server configuration, see *Avaya Aura® Communication Manager System Capacities Table*, 03-300511.) Assigns the location number to a particular station. Allows IP telephones and softphones connected through a VPN to be associated with the branch an employee is assigned to. This field is one way to associate a location with a station. For the other ways and for a list of features that use location, see the Location sections in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.
blank	Indicates that the existing location algorithm applies. By default, the value is blank.

Active Station Ringing

Defines how calls ring to the telephone when it is off-hook without affecting how calls ring at this telephone when the telephone is on-hook.

Valid Entry	Usage
continuous	All calls to this telephone ring continuously.
single	Calls to this telephone receive one ring cycle and then ring silently.
if-busy-single	Calls to this telephone ring continuously when the telephone is off-hook and idle. Calls to this telephone receive one ring cycle and then ring silently when the telephone is off-hook and active.
silent	All calls to this station ring silently.

Auto Answer

In EAS environments, the auto answer setting for the Agent LoginID can override a station's setting when an agent logs in.

Valid Entry	Usage
all	All ACD and non-ACD calls terminated to an idle station cut through immediately. Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when the **Allow Ringer-off with Auto-Answer** is enabled for the system.
acd	Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls terminated to a station ring audibly. For analog stations, the station is off-hook and idle, only the ACD split/ skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the station is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone.
none	All calls terminated to this station receive an audible ringing treatment.

Valid Entry	Usage
icom	A telephone user can answer an intercom call from the same intercom group without pressing the **intercom** button.

MWI Served User Type

Controls the auditing or interrogation of a served user's message waiting indicator (MWI).

Valid Entries	Usage
fp-mwi	The station is a served user of an fp-mwi message center.
qsig-mwi	The station is a served user of a qsig-mwi message center.
blank	The served user's MWI is not audited or if the user is not a served user of either an fp-mwi or qsig-mwi message center.

Coverage After Forwarding

Governs whether an unanswered forwarded call is provided coverage treatment.

Valid Entry	Usage
y	Coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters.
n	No coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters.
s(ystem)	Administered system-wide coverage parameters determine treatment.

Per Station CPN - Send Calling Number

Determines Calling Party Number (CPN) information sent on outgoing calls from this station.

Valid Entries	Usage
y	All outgoing calls from the station deliver the CPN information as "Presentation Allowed."
n	No CPN information is sent for the call.
r	Outgoing non-DCS network calls from the station delivers the Calling Party Number information as "Presentation Restricted."
blank	The sending of CPN information for calls is controlled by administration on the outgoing trunk group the calls are carried on.

Display Language

Valid Entry	Usage
english french italian spanish user-defined	The language that displays on stations. Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.).

Valid Entry	Usage
unicode	Displays English messages in a 24-hour format . If no Unicode file is installed, displays messages in English by default. **Note:** Unicode display is only available for Unicode-supported telephones. Currently, 4610SW, 4620SW, 4621SW, 4622SW, 16xx, 96xx, 96x1, and 9600-series telephones (Avaya one-X Deskphone Edition SIP R2 or later) support Unicode display. Unicode is also an option for DP1020 (aka 2420J) and SP1020 (Toshiba SIP Phone) telephones when enabled for the system.

Personalized Ringing Pattern

Defines the personalized ringing pattern for the station. Personalized Ringing allows users of some telephones to have one of 8 ringing patterns for incoming calls. For virtual stations, this field dictates the ringing pattern on its mapped-to physical telephone.

L = 530 Hz, M = 750 Hz, and H = 1060 Hz

Valid Entries	Usage
1	MMM (standard ringing)
2	HHH
3	LLL
4	LHH
5	HHL
6	HLL
7	HLH
8	LHL

Hunt-to Station

The extension the system must hunt to for this telephone when the telephone is busy. You can create a station hunting chain by assigning a hunt-to station to a series of telephones.

Remote Softphone Emergency Calls

Tells Communication Manager how to handle emergency calls from the IP telephone.

Caution:

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. You cannot use an Avaya IP endpoint to dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. Avoid using an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your

use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones.

Available only if the station is an IP Softphone or a remote office station.

Valid Entry	Usage
as-on-local	If the emergency location extension that corresponds to this station's IP address is not administered (left blank), the value as-on-local sends the station emergency location extension to the Public Safety Answering Point (PSAP). If the administrator populates the IP address mapping with emergency numbers, the value as-on-local functions as follows: • If the station emergency location extension is the same as the IP address mapping emergency location extension, the value as-on-local sends the station's own extension to the Public Safety Answering Point (PSAP). • If the station emergency location extension is different from the IP address mapping emergency location extension, the value as-on-local sends the IP address mapping extension to the Public Safety Answering Point (PSAP).
block	Prevents the completion of emergency calls. Use this entry for users who move around but always have a circuit-switched telephone nearby, and for users who are farther away from the server than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP Telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.
cesid	Allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. The end user enters the emergency information into the IP Softphone. Use this entry for IP Softphones with road warrior service that are near enough to the server that an emergency call reaches the PSAP that covers the softphone's physical location. If the server uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the server uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP Softphone location, based on advice from the local emergency response personnel.
option	Allows the user to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported. This entry is used for extensions that can be swapped back and forth between IP Softphones and a telephone with a fixed location. The user chooses between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects the extension.

Service Link Mode

Determines the duration of the service link connection. The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and a server running Avaya Communication Manager that terminates the H.320 protocol. When the user receives or makes a call during a multimedia or IP Softphone or IP Telephone session, a "service link" is established.

Valid Entry	Usage
as-needed	Used for most multimedia, IP Softphone, or IP Telephone users. Setting the **Service Link Mode** to as-needed leaves the service link connected for 10 seconds after the user ends a call so that they can immediately place or take another call. After 10 seconds, the link is drops. A new link need to be established to place or take another call.
permanent	Used for busy call center agents and other users who are constantly placing or receiving multimedia, IP Softphone, or IP Telephone calls. In permanent mode, the service link stays up for the duration of the multimedia, IP Softphone, or IP Telephone application session.

Loss Group

Valid Entry	Usage
1 to 17	Determines which administered two-party row in the loss plan applies to each station. Is not displayed for stations that do not use loss, such as x-mobile stations and MASI terminals.

Speakerphone

Controls the behavior of speakerphones.

Valid Entry	Usage
1-way	Indicates that the speakerphone listen-only.
2-way	Indicates that the speakerphone is both talk and listen.
grp-listen	With Group Listen, a telephone user can talk and listen to another party with the handset or headset while the telephone's two-way speakerphone is in the listen-only mode. Others in the room can listen, but cannot speak to the other party through the speakerphone. The person talking on the handset acts as the spokesperson for the group. Group Listen provides reduced background noise and improves clarity during a conference call when a group needs to discuss what is being communicated to another party. Available only with 6400-series and 2420/2410 telephones.
none	Not administered for a speakerphone.

LWC Reception

Indicates where Leave Word Calling (LWC) messages are stored.

Valid Entry	Usage
audix	LWC messages are stored on the voice messaging system.
none	LWC messages are not be stored.
spe	LWC messages are stored in the system or on the switch processor element (spe).

Survivable COR

Sets a level of restriction for stations to be used with the survivable dial plan to limit certain users to only to certain types of calls. You can list the restriction levels in order from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by PIM module of the Integrated Management to communicate with the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for Standard Local Survivability (SLS) on the Branch Gateways.

Available for all analog and IP station types.

Valid Entries	Usage
emergency	This station can only be used to place emergency calls.
internal	This station can only make intra-switch calls. This is the default.
local	This station can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.
toll	This station can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables.
unrestricted	This station can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users.

Time of Day Lock Table

Valid Entry	Usage
1 to 5	Assigns the station to a Time of Day (TOD) Lock/Unlock table. The assigned table must be administered and active.
blank	Indicates no TOD Lock/Unlock feature is active. This is the default.

Survivable GK Node Name

Any valid previously-administered IP node name. Identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the Branch Gateways. When a valid IP node name is entered into this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP stations register with Communication Manager, this list is sent down in the registration confirm message. With this, the IP station can use the IP address of this Survivable Gatekeeper as the call controller of last resort.

If blank, there are no external gatekeeper nodes within a customer's network. This is the default value.

Available only if the station type is an H.323 station for the 46*xx* or 96*xx* models.

Media Complex Ext

When used with Multi-media Call Handling, indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to place either a voice or a data call, and voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.

Valid Entry	Usage
A valid BRI data extension	For MMCH, enter the extension of the data module that is part of this multimedia complex.
H.323 station extension	For 4600 series IP Telephones, enter the corresponding H.323 station. For IP Softphone, enter the corresponding H.323 station. If you enter a value in this field, you can register this station for either a road-warrior or telecommuter/Avaya IP Agent application.
blank	Leave this field blank for single-connect IP applications.

AUDIX Name

The voice messaging system associated with the station. Must contain a user-defined adjunct name that was previously administered.

Call Appearance Display Format

Specifies the display format for the station. Bridged call appearances are not affected by this field. This field is available only on telephones that support downloadable call appearance buttons, such as the 2420 and 4620 telephones.

Note:

This field sets the administered display value only for an individual station.

Valid Entry	Usage
loc-param-default	The system uses the administered system-wide default value. This is the default.
inter-location	The system displays the complete extension on downloadable call appearance buttons.
intra-location	The system displays a shortened or abbreviated version of the extension on downloadable call appearance buttons.

IP Phone Group ID

Available only for H.323 station types.

Valid Entry	Usage
0 to 999 blank	The Group ID number for this station.

Always Use

Enables or disables the following emergency call handling settings:

- A softphone can register no matter what emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the administered **Emergency Location Extension** is used. The user-entered settings of the softphone are ignored.
- If an IP telephone dials 911, the administered **Emergency Location Extension** is used.
- If a call center agent dials 911, the physical station extension is displayed, overriding the administered **LoginID for ISDN Display**.

Does not apply to SCCAN wireless telephones, or to extensions administered as type h.323.

Audible Message Waiting

Enables or disables an audible message waiting tone indicating the user has a waiting message consisting of a stutter dial tone when the user goes off-hook.

This field does *not* control the Message Waiting lamp.

Available only if **Audible Message Waiting** is enabled for the system.

Auto Select Any Idle Appearance

Enables or disables automatic selection of any idle appearance for transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Communication Manager selects the first idle appearance.

Bridged Call Alerting

Controls how the user is alerted to incoming calls on a bridged appearance.

Valid Entry	Usage
y	The bridged appearance rings when a call arrives at the primary telephone.
n	The bridged appearance flashes but does not ring when a call arrives at the primary telephone. This is the default. If disabled and **Per Button Ring Control** is also disabled, audible ringing is suppressed for incoming calls on bridged appearances of another telephone's primary extension.

Bridged Idle Line Preference

Specifies whether the selected line for incoming bridged calls is always an idle line.

Valid Entry	Usage
y	The user connects to an idle call appearance instead of the ringing call.
n	The user connects to the ringing call appearance.

CDR Privacy

Enables or disables Call Privacy for each station. With CDR Privacy, digits in the called number field of an outgoing call record can be blanked on a per-station basis. The number of blocked digits is administered system-wide as CDR parameters.

Conf/Trans On Primary Appearance

Enables or disables the forced use of a primary appearance when the held call to be conferenced or transferred is a bridge. This is regardless of the administered value for **Auto Select Any Idle Appearance** .

Coverage Msg Retrieval

Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.

IP Video

Enables or disables IP video capability for this signaling group. Available only if the signaling group type h.323 and sip.

Data Restriction

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

Direct IP-IP Audio Connections

Supports or prohibits direct audio connections between IP endpoints that saves on bandwidth resources and improves sound quality of voice over IP transmissions.

Display Client Redirection

Enables or disables the display of redirection information for a call originating from a station with Client Room Class of Service and terminating to this station. When disabled, only the client name and extension or room display. Available only if Hospitality is enabled for the system.

Note:

This field must be enabled for stations administered for any type of voice messaging that needs display information.

Select Last Used Appearance

Valid Entry	Usage
y	Indicates a station's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. The line selection on an on-hook station only moves from the last used line button to a line button with an audibly alerting call. If there are no alerting calls, the line selection remains on the button last used for a call.
n	The line selection on an on-hook station with no alerting calls can be moved to a different line button that might be serving a different extension.

Survivable Trunk Dest

Designates certain telephones as not being allowed to receive incoming trunk calls when the Branch Gateway is in survivable mode. This field is used by the PIM module of the Integrated Management to successfully interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the Branch Gateways.

Available for all analog and IP station types.

Valid Entry	Usage
y	Allows this station to be an incoming trunk destination while the Branch Gateway is running in survivability mode. This is the default.
n	Prevents this station from receiving incoming trunk calls when in survivable mode.

H.320 Conversion

Enables or disables the conversion of H.320 compliant calls made to this telephone to voice-only. The system can handle only a limited number of conversion calls. Therefore, the number of telephones with H.320 conversion must be limited.

Idle Appearance Preference

Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.

Valid Entry	Usage
y	The user connects to an idle call appearance instead of the ringing call.
n	The Alerting Appearance Preference is set and the user connects to the ringing call appearance.

IP Audio Hairpinning

Enables or disables hairpinning for H.323 or SIP trunk groups. H.323 and SES-enabled endpoints are connected through the IP circuit pack without going through the time division multiplexing (TDM) bus. Available only if **Group Type** is h.323 or sip.

IP Softphone

Indicates whether or not this extension is either a PC-based multifunction station or part of a telecommuter complex with a call-back audio connection.

Available only for DCP station types and IP Telephones.

LWC Activation

Activates or deactivates the Leave Word Calling (LWC) feature. With LWC, internal telephone users on this extension can leave short pre-programmed messages for other internal users.

You must use LWC if:

- The system has hospitality and the guest-room telephones require LWC messages indicating that wakeup calls failed
- The LWC messages are stored in a voice-messaging system

LWC Log External Calls

Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls provided information on the caller identification is available. Each record consists of the latest call attempt date and time.

Multimedia Early Answer

Enables or disables multimedia early answer on a station-by-station basis.

You must enable the station for the Multimedia Early Answer feature if the station receives coverage calls for multimedia complexes, but is not multimedia-capable. This ensures that calls are converted and the talk path is established before ringing at this station.

Mute Button Enabled

Enables or disables the mute button on the station.

Per Button Ring Control

Enables or disables per button ring control by the station user.

Valid Entries	Usage
y	Users can select ring behavior individually for each call-appr, brdg-appr, or abrdg-appr on the station and to enable Automatic Abbreviated and Delayed ring transition for each call-appr on the station. Prevents the system from automatically moving the line selection to a silently alerting call unless that call was audibly ringing earlier.
n	Calls on **call-appr** buttons always ring the station and calls on **brdg-appr** or **abrdg-appr** buttons always ring or not ring based on the **Bridged Call Alerting** value. The system can move line selection to a silently alerting call if there is no call audibly ringing the station.

Precedence Call Waiting

Activates or deactivates Precedence Call Waiting for this station.

Redirect Notification

Enables or disables redirection notification that gives a half ring at this telephone when calls to this extension are redirected through Call Forwarding or Call Coverage. Must be enabled if LWC messages are stored on a voice-messaging system.

Restrict Last Appearance

Valid Entries	Usage
y	Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only.
n	Last idle call appearance is used for incoming priority calls and outgoing call originations.

EMU Login Allowed

Enables or disables using the station as a visited station by an Enterprise Mobility User (EMU).

Bridged Appearance Origination Restriction

Restricts or allows call origination on the bridged appearance.

Valid Entry	Usage
y	Call origination on the bridged appearance is restricted.
n	Call origination ion the bridged appearance is allowed. This is normal behavior, and is the default.

Voice Mail Number

Displays the complete voice mail dial up number. Accepts a value of up to 24 characters consisting of digits from 0 to 9, asterisk (*), pound sign (#), ~p (pause), ~w/~W (wait), ~m (mark), and ~s (suppress). This field is supported in the following set types: 9620SIP, 9630SIP, 9640SIP, 9650SIP, 9608SIP, 9611SIP, 9621SIP, 9641SIP, 9608SIPCC, 9611SIPCC, 9621SIPCC, and 9641SIPCC.

Site Data

This section lets you set information about the Room, Floor, Jack, Cable, Mounting, and Building.

Room

Valid Entry	Usage
Telephone location	Identifies the telephone location. Accepts up to 10 characters.
Guest room number	Identifies the guest room number if this station is one of several to be assigned a guest room and the **Display Room Information in Call Display** is enabled for the system. Accepts up to five digits.

Floor

A valid floor location.

Jack

Alpha-numeric identification of the jack used for this station.

Cable

Identifies the cable that connects the telephone jack to the system.

Mounting

Indicates whether the station mounting is d(esk) or w(all).

Building

A valid building location.

Set Color

Indicates the set color. Valid entries include the following colors: beige, black, blue, brown, burg (burgundy), gray, green, ivory, orng (orange), red, teak, wal (walnut), white, and yel (yellow).

You can change the list of allowed set colors by using the Valid Set Color fields on the site-data screen.

Cord Length

The length of the cord attached to the receiver. This is a free-form entry, and can be in any measurement units.

Headset

Indicates whether or not the telephone has a headset.

Speaker

Indicates whether or not the station is equipped with a speaker.

Abbreviated Call Dialing

This section lets you create abbreviated dialing lists for a specific station, and provide lists of stored numbers that can be accessed to place local, long-distance, and international calls; allows you to activate features or access remote computer equipment and select enhanced, personal, system or group lists.

Abbreviated Dialing List 1, List 2, List 3

Assigns up to three abbreviated dialing lists to each telephone.

Valid Entry	Usage
enhanced	Telephone user can access the enhanced system abbreviated dialing list.
group	Telephone user can access the specified group abbreviated dialing list. Requires administration of a group number.
personal	Telephone user can access and program their personal abbreviated dialing list. Requires administration of a personal list number.
system	Telephone user can access the system abbreviated dialing list.

Personal List

Establishes a personal dialing list for telephone or data module users. The personal list must first be assigned to the telephone by the System Administrator before the telephone user can add entries in the list. Users access the lists to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Abbreviated Dialing Enhanced List

Establishes system-wide or personal lists for speed dialing.

The Enhanced Abbreviated Dialing List can be accessed by users to place local, long-distance, and international calls; to activate or deactivate features; or to access remote computer equipment.

Note:

Dialing must be activated in the license file before the Enhanced List can be programmed.

Group List

Implements the Abbreviated Dialing Group List. The System Administrator controls the Group Lists. Up to 100 numbers can be entered for every group list. Users can access this list to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Enhanced Call Fwd

This section allows you to specify the destination extension for the different types of call forwards.

Forwarded Destination

A destination extension for both internal and external calls for each of the three types of enhanced call forwarding (Unconditional, Busy, and No Reply). Accepts up to 18 digits. The first digit can be an asterisk *.

Requires administration to indicate whether the specific destination is active (enabled) or inactive (disabled).

SAC/CF Override

With **SAC/CF Override**, the user of a station with a **Team** button administered, who is monitoring another station, can directly reach the monitored station by pushing the **Team** button. This overrides any currently active rerouting, such as Send All Calls and Call Forwarding, on the monitored station.

Valid Entries	Usage
Ask	The system asks if the user wants to follow the rerouting or override it. When the user has the option to decide whether rerouting must take place

Valid Entries	Usage
	or not, a message is sent to the station that displays the active rerouting and the number of the forwarded to station.
No	Cannot override rerouting. The station does not have the ability to override the rerouting of a monitored station.
Yes	Can override rerouting. The station can override the rerouting the monitored station has set, as long as one incoming call appearance is free.

Button Assignment

This section lets you assign features to the buttons on a phone. You can assign the main buttons for your station by choosing an option from the list down box for each button.

Group Membership

This section describes the different groups that an extension can be a member of. Select the station you want to group, and then choose the group from the drop-down box, before you click **Commit**.

Understanding groups

Your voice system uses groups for a number of different purposes. This topic describes the different groups that an extension can be a member of. However, your voice system might include other types of groups such as trunk groups. For more information on groups, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Your voice system can have any of the following types of groups set up:

Type	Description
group page	Group page is a feature that allows you to make an announcement to a pre-programmed group of phone users. The announcement is heard through the speakerphone built into some sets. Users will hear the announcement if their set is idle. Users cannot respond to the announcement.
coverage answer group	A coverage answer group lets up to 8 phones ring simultaneously when a call is redirected to the group.
coverage path	A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call. For more information on coverage paths, see “Creating Coverage Paths” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
hunt group	A hunt group is a group of extensions that receive calls according to the call distribution

Type	Description
	method you choose. When a call is made to a certain phone number, the system connects the call to an extension in the group. Use hunt groups when you want more than one person to be able to answer calls to the same number. For more information on hunt groups, see “Managing Hunt Groups” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
intercom group	An intercom group is a group of extensions that can call each other using the intercom feature. With the intercom feature, you can allow one user to call another user in a predefined group just by pressing a couple of buttons. For more information on intercom groups, see “Using Phones as Intercoms” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
pickup group	A pickup group is a group of extensions in which one person can pick up calls of another person. For more information on pickup groups, see “Adding Call Pickup” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
terminating extension group	A Terminating Extension Group (TEG) allows an incoming call to ring as many as 4 phones at one time. Any user in the group can answer the call. For more information on terminating extension groups, see “Assigning a Terminating Extension Group” in the *Administering Avaya Aura® Communication Manager, 03-300509*.

Edit Endpoint Extension field descriptions

Use this page to change the extension of an endpoint.

Field	Description
System	Specifies the list of Communication Managers. Select one of the options.

Field	Description
Extension	Extension of the device you want to change.
New Extension	New extension you want to provide for the device.
Emergency location extension	Existing emergency location extension of your device.
New emergency location extension	New existing emergency location extension you want to provide.
Message lamp extension	Existing message lamp extension of your device.
New message lamp extension	New message lamp extension you want to provide.

Button	Description
Commit	Saves the new extension.
Schedule	Saves the extension at the scheduled time.
Reset	Clears all the entries.
Cancel	Takes you back to the previous page.

Bulk Add Endpoint field descriptions

Field	Description
Template	The template you choose for the endpoints.
Station name prefix	Specifies the prefix name that the system displays for each of the endpoints you add. You can enter a prefix name of your choice in this field.
System	Specifies the list of the Communication Managers.
Available extensions	The list of extensions that are available.
Enter extensions	The extensions that you want to use. You can enter your preferred extensions in this field.

Button	Description
Commit	Bulk adds the endpoints.
Schedule	Bulk adds the station at the scheduled time.

Button	Description
Clear	Undoes all the entries.
Cancel	Takes you to the previous page.

Bulk Edit Endpoint field descriptions

Name	Description
Template	Specifies the endpoint template. You can choose the template which you want to bulk edit.
Station Name Prefix	Specifies the prefix name which the system displays before all the endpoints that you bulk edit. You can enter a prefix name of your choice.

Button	Description
Commit	Bulk edits the endpoints.
Schedule	Bulk edits the endpoints at the specified time.
Clear	Undoes the entries.
Cancel	Takes you to the previous page.

Swap Endpoints field descriptions

Name	Description
Assign data for Endpoint <*n*>	Provides the option to assign new values of location site data to the respective endpoint. When you select this check box for an endpoint, then the location site data values of this endpoint is copied to the second endpoint where this check box is clear. If you select the check boxes for both the endpoints, then it equates to copying new location site data to respective endpoints. No swapping takes place.
System	Specifies the Communication Manager that the endpoint is assigned to. This will show

Name	Description
	the selection from Communication Manager List page.
Endpoint 1 **Endpoint 2**	Displays the existing endpoint extension number on the selected System .

Button	Description
Commit	Performs the action you initiate.
Schedule	Performs the action at the specified time.
Cancel	Cancels your current action and takes you to the previous page.

Error codes

Following table gives the common error codes for Busyout, Release, Test, and Reset Commands lists. This table also has the common error codes associated with abort and fail results for busyout, release, test, and reset commands. In addition to these, many maintenance objects have other unique error codes.

Error Code	Command Result	Description/Recommendation
	ABORT	System resources are unavailable to run command. Try the command again at 1-minute intervals up to 5 times.
0	ABORT	Internal system error. Retry the command at 1-minute intervals up to 5 times.
1005	ABORT	A DS1 interface circuit pack could not be reset because it is currently supplying the on-line synchronization reference. Use set sync to designate a new DS1 interface circuit pack as the on-line reference, then try the reset again.
1010	ABORT	Attempt was made to busyout an object that was already busied out.
1011	ABORT	Attempt was made to release an object that was not first busied out.
1015	ABORT	A reset of this circuit pack requires that every maintenance object on it be in the out-of-service state. Use busyout board to place every object on the circuit pack in the out-of-service state, and try the reset again.
1026	ABORT	The specified TDM bus cannot be busied out because the control channel or system tones are being carried on it. Use set tdm PC to switch the control channel and system tones to the other TDM bus.

2012 2500	ABORT	Internal system error.
2100	ABORT	System resources to run this command were unavailable. Try the command again at 1-minute intervals up to 5 times.
62524 62525 62526	ABORT	Maintenance is currently active on the maximum number of maintenance objects that the system can support. A common cause is that the system contains a large number of administered stations or trunks with installed circuit packs that are not physically connected. Resolve as many alarms as possible on the station and trunk MOs, or busyout these MOs to prevent maintenance activity on them. Then try the command again.
	NO BOARD	The circuit pack is not physically installed.
2100	EXTRA BD	This result can appear for: S8700 Maintenance/Test, Announcement circuit packs S8700 MC Call Classifier, Tone Detector, Speech Synthesis circuit packs Each of these circuit packs has restrictions on how many can be installed in the system or in a port network, depending on system configuration. Remove any extra circuit packs.
1	FAIL	For reset commands, the circuit pack was not successfully halted.
2	FAIL	For reset commands, the circuit pack was not successfully restarted after being halted. For both results replace the circuit pack.
	FAIL	See the applicable maintenance object (from the Maintenance Name field) in Maintenance Alarms Reference, 03-300190.
	PASS	The requested action successfully completed. If the command was a reset, the circuit pack is now running and should be tested.

Xmobile Configuration

Xmobile Configuration

Xmobile Configuration defines the number of call treatment options for Extension to Cellular calls for cellular telephones. The Extension to Cellular feature allows the use of up to 99 Configuration Sets, already defined in the system using default values.

Xmobile Configuration List

Xmobile Configuration List displays the Xmobile Configuration details under the Communication Manager you select. You can apply filters and sort each column in this list.

Click **Refresh** to view the updated information after the last synchronization.

Name	Description
Configuration Set	Displays the configuration set value.
Calling No.	Displays the format of the caller ID for calls from a local switch extension to an EC500 cell phone.
CDR Orig	Displays the CDR report format when CDR records are generated for a call that originates from an Extension to Cellular cell phone.
CDR EC 500	Displays whether a call detail record is generated for any call to the cell phone.
Fast Conn	Displays whether some additional processing occurs on the switch prior to connecting a call.
Post-Connect Dialing	Displays whether additional capabilities, beyond standard ISDN dialing, are available for those incoming ISDN trunk calls that are mapped into XMOBILE stations.
System	Specifies the name of the Communication Manager associated with the Xmobile Configuration set.

Viewing Xmobile Configuration data

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Xmobile Configuration**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Xmobile Configuration List, select the configuration set you want to view.

6. Click **View**.

Related topics:

Xmobile Configuration field descriptions on page 575

Editing Xmobile Configuration

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Xmobile Configuration**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Xmobile Configuration List, select the configuration set you want to view.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required details on the **Edit Xmobile Configuration Data** page.
8. Click **Commit** to save the changes.

Related topics:

Xmobile Configuration field descriptions on page 575

Xmobile Configuration field descriptions

Field	Description
Barge-in Tone	Enables a barge-in tone used to add security to Extension to Cellular calls. If a user is on an active Extension to Cellular call and another person joins the call from an Extension to Cellular enabled office telephone, all parties on the call hear the barge-in tone.

Field	Description
Calling Number Style	Determines the format of the caller ID for calls from a local switch extension to an EC500 cell phone. • **network**: Provides a display of only 10-digit numbers. For internal calls, the ISDN numbering tables are used to create the calling number and DCS calls use the ISDN calling number if provided. The externally provided calling number is used when available for externally originated calls. • **pbx**: Provides a display of less than 10-digits. Extensions sent as the calling number for all internally- and DCS network-originated calls.
CDR for Calls to EC500 Destination	Determines whether a call detail record is generated for calls to the cell phone. **Note:** CDR reporting for EC500 calls relies on the CDR Reports field on the Trunk Group screen. If, on the Trunk Group screen, the CDR Reports field is set to **n**, no CDR is generated even if this field is set to **y**. • **y**: Treats calls to the XMOBILE station as trunk calls and generates a CDR. • **n**: Treats calls to the XMOBILE station as internal calls and does not generate a CDR.
Configuration Set Description	Describes the purpose of the configuration set. A valid entry is up to 20 alphanumeric characters or blank. For example, EC500 handsets.
Fast Connect on Origination	Determines whether some additional processing occurs on the switch prior to connecting a call. You can use the **y** option to send CONNECT messages.
Post-Conn Signaling	Post Connect Dialing Options. Determines whether additional capabilities, beyond standard ISDN dialing, are available for those incoming ISDN trunk calls that are mapped into XMOBILE stations. These options come into effect after the call has entered the active state when the switch has

Field	Description
	sent a CONNECT message back to the network. • **dtmf**: Expect digits from either in-band or out-of-band, but not simultaneously. The switch allocates a DTMF receiver whenever it needs to collect digits. This option is generally used for EC500 XMOBILE station calls. • **out-of-band**: Expect all digits to be delivered by out-of-band signaling only. The switch collects digits that it needs from the out-of-band channel (no touch-tone receiver). In addition, any digits received when the switch is not collecting digits are converted to DTMF and broadcast to all parties on the call. This option is in force for DECT XMOBILE station calls. • **both**: Expect all subsequent digits to be delivered by simultaneous in-band and out-of-band signaling. Out-of-band signaling consists of digits embedded in ISDN INFO messages while the in-band signaling consists of DTMF in the voice path. The switch collects all digits that it needs from the out-of-band channel. No touch tone receive is allocated in order to prevent collecting double digits. End-to-end signaling occurs transparently to the switch through in-band transmission of DTMF. This option is in force for PHS XMOBILE station calls.
Call Appearance Selection for Origination	Specifies how the system selects a Call Appearance for call origination. To use this feature, bridged calls must be enabled for the system. • **first-available**: The system searches for the first available regular or bridged Call Appearance. • **primary-first**: Only regular Call Appearances are used for call origination. If a regular call appearance is not available, the call is not allowed. The system first searches for a regular Call Appearance for call origination. If a regular Call Appearance is not available, a second search is made that includes both regular

Field	Description
	and bridged Call Appearances. This is the default setting.
Calling Number Verification	Enables restrictions on the types of calls made to a cell phone with Extension to Cellular. • **y**: Prevents all calls, except for the following calls, from reaching the cell phone: - Network-provided - User-provided - Passed This setting has no effect on normal usage of the Extension to Cellular feature. This is the default setting. • **n**: No restrictions on calls to the cell phone.
CDR for Origination	Determines the CDR report format when CDR records are generated for a call that originates from an Extension to Cellular cell phone. To generate this CDR, you must enable the Incoming Trunk CDR. The CDR report does not include dialed Feature Name Extensions (FNEs). • **phone-number**: The calling party on the CDR report is the 10-digit cell phone number. This is the default setting. • **extension**: The calling party on the CDR report is the internal office telephone phone extension associated with the Extension to Cellular cell phone. • **none**: The system does not generate an originating CDR report.
Cellular Voice Mail Detection	Prevents cellular voice mail from answering an Extension to Cellular call. The call server detects when the cell phone is not the entity that answers the call and brings the call back to the server. Communication Manager treats the call as a normal call to the office telephone and the call goes to corporate voice mail. You can also set a timer for cellular voice mail detection that sets a time

Field	Description
	before Cellular Voice Mail Detection investigates a call. • **none**: No restrictions on cellular voice mail. This is the default setting. • **timed**: Amount of time from 1 to 9 seconds. The default time is 4 seconds. Extension to Cellular call leg answered within the specified time is detected as being answered by the cellular voice mail and the call continues to ring at the office telephone. If unanswered, it will go to the corporate voice mail. This setting can be used for different types of network that is, GSM, CDMA, and ISDN. • **message**: The message option works with carriers who use non ISDN voice mail systems. Avoid using this option with ISDN-based voice mail systems.
Confirmed Answer	Enables Confirmed Answer on Extension to Cellular calls for this station. If you select this option, the user needs to input a digit to confirm receipt of a call sent to a cell phone using the Extension to Cellular feature. When the user answers the incoming call on the cell phone, the user hears a dial tone. The user must then press any one of the digits on the cell phone keypad. Until the system receives a digit, the system does not treat the call as answered. The length of time to wait for the digit can be administered from 5 to 20 seconds, with a default of 10 seconds. The system plays a recall dial tone to indicate that input is expected. During the response interval, the original call continues to alert at the desk phone and any stations bridged to the call. If the user does not enter a digit before the time-out interval expires, the call is pulled back from the telephone device.
Configuration Set ID	Displays the configuration set value that you selected in the Xmobile Configuration List. This is a display-only field.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.

Button	Description
Reset	Clears the action and resets the field.
Clear	Clears all the entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Automatic Alternate Routing Digit Conversion

AAR/ARS Digit Conversion

Use the Automatic Alternate Routing (AAR) Digit Conversion or Automatic Route Selection (ARS) Digit Conversion capability to configure your system to change a dialed number for efficient routing by inserting or deleting digits from the dialed number. For instance, you can configure the server running Communication Manager to delete **1** and an area code on calls to one of your locations, and avoid long-distance charges by routing the call over your private network.

Viewing Automatic Alternate Routing Digit Conversion data

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Alternate Routing Digit Conversion**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the AAR Digit Conversion List, select the Automatic Alternate Routing Digit Conversion data you want to view.
6. Click **View**.

Related topics:

AAR/ARS Digit Conversion field descriptions on page 581

Editing Automatic Alternate Routing Digit Conversion data

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Alternate Routing Digit Conversion**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the AAR Digit Conversion List, select the Automatic Alternate Routing Digit Conversion you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit AAR Digit Conversion** page.
8. Click **Commit** to save the changes.

Related topics:

AAR/ARS Digit Conversion field descriptions on page 581

AAR/ARS Digit Conversion field descriptions

Field	Description
ANI Required	This field applies only if the Request Incoming ANI (non-AAR/ARS) field on the Multifrequency-Signaling-Related System Parameters screen is set to n. • **y** or **n**: Enter y to require ANI on incoming R2-MFC or Russian MF ANI calls. The entry must be set to y to enable EC500 origination features. • **r**: Restricted. Allowed only if the Allow ANI Restriction on AAR/ARS field is set to y on the Feature-Related System Parameters screen. Use this entry to drop a call on a Russian Shuttle trunk or Russian Rotary

Field	Description
	trunk if the ANI request fails. Other types of trunks treat **r** as **y**.
Conv	Provides the option to allow additional digit conversion.
Del	Displays the number of digits you want the system to delete from the beginning of the dialed string. A valid entry ranges from **0** to **Min**.
Location	This is a display-only field. Typing the command `change aar digit-conversion` *n* or `change ars digit-conversion` *n* displays the all-locations screen, and populates this field with **all**. The *n* specifies that dialed strings beginning with the value *n* are displayed first. To access a per-location screen, type change `aar digit-conversion location` *n* or `change ars digit-conversion location` *n*, where *n* represents the number of a specific location. This field then displays the number of the specified location. For details on command options, see online help, or *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431. One of the following is a valid entry: • **1** to **64**: Specifies whether you require ANI on incoming R2-MFC or Russian MF ANI calls. Entry must be `y` to enable EC500 origination features. • **all**: Indicates that this AAR/ARS Digit Conversion Table is the default for all port network (cabinet) locations.
Matching Pattern	Specifies the number you want the server running Communication Manager to match to dialed numbers. If a prefix digit **1** is required for 10-digit direct distance dialing (DDD) numbers, be sure the matching pattern begins with a 1. A valid entry is a number ranging from **0** to **9** (1 to 18 digits) and wildcard characters asterisk (*****), **x**, and **X**.

Field	Description
Max	Specifies the maximum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from **Min** to **28**.
Min	Specifies the minimum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from **1** to **Max**.
Net	Specifies the call-processing server network used to analyze the converted number. The entries **ext**, **aar**, or **ars** analyze the converted digit-string as an extension number, an AAR address, or an ARS address.
Percent Full	Displays the percentage from **0** to **100** of the system memory resources that have been used by ARS. If the figure is close to 100 percent, you can free-up memory resources.
Replacement String	A valid entry ranges from **0** to **9** (1 to 18 digits), asterisk (*****), pound (**#**), or blank. Enter the digits that replace the deleted portion of the dialed number. If the pound character (#) is present in the string, it should be the last character in the string. This signifies the end of the modified digit string. Leave this field blank to simply delete the digits.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.
Clear	Clears all the entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Automatic Route Selection Digit Conversion

AAR/ARS Digit Conversion

Use the Automatic Alternate Routing (AAR) Digit Conversion or Automatic Route Selection (ARS) Digit Conversion capability to configure your system to change a dialed number for efficient routing by inserting or deleting digits from the dialed number. For instance, you can configure the server running Communication Manager to delete **1** and an area code on calls to one of your locations, and avoid long-distance charges by routing the call over your private network.

Viewing Automatic Route Selection Digit Conversion data

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Route Selection Digit Conversion**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the ARS Digit Conversion List, select the Automatic Route Selection Digit Conversion you want to view.
6. Click **View**.

Related topics:

AAR/ARS Digit Conversion field descriptions on page 581

Editing Automatic Route Selection Digit Conversion data

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Route Selection Digit Conversion**.
3. Select a Communication Manager from the Communication Manager list.

4. Click **Show List**.
5. Click **Edit** or click **View** > **Edit**.
6. Edit the required fields on the **Edit ARS Digit Conversion** page.
7. Click **Commit** to save the changes.

Related topics:

AAR/ARS Digit Conversion field descriptions on page 581

AAR/ARS Digit Conversion field descriptions

Field	Description
ANI Required	This field applies only if the Request Incoming ANI (non-AAR/ARS) field on the Multifrequency-Signaling-Related System Parameters screen is set to n. • **y** or **n**: Enter y to require ANI on incoming R2-MFC or Russian MF ANI calls. The entry must be set to y to enable EC500 origination features. • **r**: Restricted. Allowed only if the Allow ANI Restriction on AAR/ARS field is set to y on the Feature-Related System Parameters screen. Use this entry to drop a call on a Russian Shuttle trunk or Russian Rotary trunk if the ANI request fails. Other types of trunks treat **r** as **y**.
Conv	Provides the option to allow additional digit conversion.
Del	Displays the number of digits you want the system to delete from the beginning of the dialed string. A valid entry ranges from **0** to **Min**.
Location	This is a display-only field. Typing the command `change aar digit-conversion` *n* or `change ars digit-conversion` *n* displays the all-locations screen, and populates this field with **all**. The *n* specifies that dialed strings beginning with the value *n* are displayed first. To access a per-location screen, type

Field	Description
	change `aar digit-conversion location` *n* or `change ars digit-conversion location` *n*, where *n* represents the number of a specific location. This field then displays the number of the specified location. For details on command options, see online help, or *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431. One of the following is a valid entry: • **1** to **64**: Specifies whether you require ANI on incoming R2-MFC or Russian MF ANI calls. Entry must be `y` to enable EC500 origination features. • **all**: Indicates that this AAR/ARS Digit Conversion Table is the default for all port network (cabinet) locations.
Matching Pattern	Specifies the number you want the server running Communication Manager to match to dialed numbers. If a prefix digit **1** is required for 10-digit direct distance dialing (DDD) numbers, be sure the matching pattern begins with a 1. A valid entry is a number ranging from **0** to **9** (1 to 18 digits) and wildcard characters asterisk (*****), **x**, and **X**.
Max	Specifies the maximum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from **Min** to **28**.
Min	Specifies the minimum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from **1** to **Max**.
Net	Specifies the call-processing server network used to analyze the converted number. The entries **ext**, **aar**, or **ars** analyze the converted digit-string as an extension number, an AAR address, or an ARS address.
Percent Full	Displays the percentage from **0** to **100** of the system memory resources that have been used by ARS. If the figure is close to 100

Field	Description
	percent, you can free-up memory resources.
Replacement String	A valid entry ranges from **0** to **9** (1 to 18 digits), asterisk (*****), pound (#), or blank. Enter the digits that replace the deleted portion of the dialed number. If the pound character (#) is present in the string, it should be the last character in the string. This signifies the end of the modified digit string. Leave this field blank to simply delete the digits.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.
Clear	Clears all the entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Automatic Route Selection Toll

Automatic Route Selection Toll

With Automatic Route Selection Toll, you can specify whether calls to CO codes listed on the table are toll or non-toll calls. You can specify non-toll calls based on the last two digits of the distant-end of the trunk group.

Automatic Route Selection Toll List

Name	Description
ARS Toll Table	Displays the Automatic Route Selection Toll table number.
From Office Code, **To Office Code**	Displays the block of numbers for the associated Automatic Route Selection Toll table.
System	Specifies the name of the Communication Manager associated with the Automatic Route Selection Toll table.

Viewing Automatic Route Selection Toll data

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Route Selection Toll**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Automatic Route Selection Toll List, select the Ars Toll Table you want to view.
6. Click **View**.

Related topics:

Automatic Route Selection Toll field descriptions on page 589

Editing Automatic Route Selection Toll data

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Route Selection Toll**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Automatic Route Selection Toll List, select the Ars Toll Table you want to edit.

6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Automatic Route Selection Toll** page.
8. Click **Commit** to save the changes.

Related topics:

Automatic Route Selection Toll field descriptions on page 589

Automatic Route Selection Toll field descriptions

Field	Description
00: through **99:**	Represents the last two digits of the codes within the 100-block of numbers. Designate each as a number toll or non-toll call.
Ars Toll Table	Specifies the number of the ARS Toll table. Valid entry ranges from **2** through **9**.
Office Codes	Indicates the block of numbers. Valid entry ranges from **200** to **299** through **900** to **999**.

Button	Description
Commit	Performs the action you initiate.
Schedule	Performs the action at the specified time.
Reset	Clears the action and resets the fields.
Clear	Clears all entries.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Backup	Backs up the audio files that you select.
Now	Performs the action you initiate real time.

Data Modules

Data Modules

Use this capability to connect systems running Communication Manager with other communications equipment, changing protocol, connections, and timing as necessary. Communication Manager supports the following types of data modules:

- High speed links
- Data stands
- Modular-processor data module
- 7000-series data modules
- Modular-trunk data module
- Asynchronous Data Unit
- Asynchronous Data Module for ISDN-Basic Rate Interface telephones
- Terminal adapters

All of these data modules support industry standards and include options for setting the operating profile to match that of the data equipment.

Data Module List

Data Module List displays all the data modules under the Communication Manager you select. You can apply filters and sort each column in the Data Module List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Extension	Displays the extension assigned to the data module.
Port	Displays port location to which the selected data module is connected.
Type	Displays the type of data module.
Name	Displays the name of the user associated with the data module.
COS	Displays the desired Class Of Service.
COR	Displays the desired Class Of Restriction.
TN	Displays the tenant number which determines the music source for callers on hold.
ISN	Information Systems Network. Used with Data Line and Processor/Trunk Data Modules.

Name	Description
System	Specifies the name of the Communication Manager associated with the data module.

Adding a Data Module

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Data Modules**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select **New**.
6. Complete the **Add Data Module** page and click **Commit**.

Related topics:

Data Modules field descriptions on page 593

Viewing a Data Module

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Data Modules**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Data Modules List, select the data module you want to view.
6. Click **View**.

Related topics:

Data Modules field descriptions on page 593

Editing a Data Module

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Data Modules**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Data Modules List, select the data module you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Data Modules** page.
8. Click **Commit** to save the changes.

Related topics:

Data Modules field descriptions on page 593

Deleting Data Modules

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Data Modules**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Data Modules List, select the data modules you want to delete.
6. Click **Delete**.
7. Confirm to delete the data modules.

Related topics:

Data Modules field descriptions on page 593

Data Modules field descriptions

Field	Description
List Type	Indicates whether the type of list is group, personal, enhanced, or system type.
Special Dialing Option	Identifies the destination of all calls when this data module originates calls. The available dialing options are: • **hot-line**: Allows single-line telephone users to automatically place a call to an extension, telephone number, or Feature Access Code (FAC). • **default**: An associated Abbreviated Dialing number is dialed when the user goes off-hook and enters a carriage return following the DIAL prompt.
Personal/Group Number	Displays the identifying number the server running Communication Manager assigns to the group when it is created.
Abbreviated Dialing Dial Code (From above list)	Used with 7500, Data Line, Netcon, Processor/Trunk, Processor Interface, and World Class BRI Data Modules. System displays this field only when the Special Dialing Option field is default. When the user goes off-hook and enters a carriage return following the DIAL prompt, the system dials the abbreviated dialing number. The data call originator can also perform data-terminal dialing by specifying a dial string that may or may not contain alphanumeric names. Valid entry ranges from **0** through **999**. You need to enter a list number associated with the abbreviated dialing list.
BCC	Bearer Capability Class. A display-only field used with Data Line, Netcon, Processor Interface, Point-to-Point Protocol, Processor/Trunk (pdm selection), and System Port Data Modules. Appears when the ISDN-PRI or ISDN-BRI Trunks field is set to y on the System Parameters Customer-Options (Optional Features) screen. The value in this field corresponds to the speed setting of the data module. This field can be compared with the BCC value in an

Field	Description
	associated routing pattern when attempted calls utilizing the data module fail to complete. The BCC values must be the same. See *Generalized Route Selection in Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for a detailed description of Bearer Capability Classes (BCC) and their ability to provide specialized routing for various types of voice and data calls. The BCC value is used to determine compatibility when non-ISDN-PRI facilities are connected to ISDN facilities (ISDN-PRI Interworking). The valid entries are: • **1**: Relates to 56-bkps • **2**, **3**, **4**: Relates to 64 kbps
Broadcast Address	Used with Ethernet data modules. Does not appear for S87XX Series IP-PNC.
Connected Data Module	This is the data module extension to which the link connects. Used with Processor Interface (used with DEFINITY CSI only) data modules.
Connected to	Displays the Asynchronous Data Unit (ADU) to which the system is connected to. Used with Data Line and Processor/Trunk (pdm selection) Data Module. The valid entries are: • **dte**: Data Terminal Equipment. Used with Data Line and Processor/Trunk Data Modules. • **isn**: Information Systems Network. Used with Data Line and Processor/Trunk Data Modules.
Class Of Service	Specifies the desired class of service. Does not appear for Ethernet. The valid entries range from **0** to **15** to select the allowed features
Class Of Restriction	Specifies the desired class of restriction. Does not appear for Ethernet. The valid entries range from **0** to **999** to select the allowed restrictions.
Extension	Indicates the extension assigned to the data module. This is a display-only field.

Field	Description
Enable Link	Used with Point-to-Point and Processor Interface data modules.
Establish Connection	Used with Point-to-Point, and Processor Interface (used with DEFINITY CSI only) data modules.
IP Address Negotiation	Used with Point-to-Point data modules. Does not appear for S87XX Series IP-PNC.
ITC	Information Transfer Capability. Indicates type of transmission facilities to be used for ISDN calls originated from this endpoint. Appears only when, on the Trunk Group screen, the Comm Type field is 56k-data or 64k-data. Does not display for voice-only or BRI stations. Used with 7500, Announcement, data-line, Netcon, Processor/Trunk (pdm selection), Processor Interface, and System Port Data Modules. The valid entries are: • **restricted**: Either restricted or unrestricted transmission facilities are used to complete the call. A restricted facility is a transmission facility that enforces 1's density digital transmission (that is, a sequence of eight digital zeros is converted to a sequence of 7 zeros and a digital 1). • **unrestricted**: Only unrestricted transmission facilities are used to complete the call. An unrestricted facility is a transmission facility that does not enforce 1's density digital transmission (that is, digital information is sent exactly as is).
Link	Displays a communication interface link number. Used with Ethernet, Point-to-Point, and Processor Interface (used with DEFINITY CSI only) data modules. This field is in different locations on the screen for different data module types. The valid entries range from **0** to **99**.
Extension	Displays the extension number required to perform maintenance functions on the standby Netcon physical channel in a duplicated system. The standby remote loop around tests fails if this field is not administered. Used with Netcon and Processor Interface Data Modules.

Field	Description
MM Complex Voice Ext	This field contains the number of the associated telephone in the multimedia complex. This field appears only after you set the Multimedia field toy. This field is left blank until you enter the data module extension in MM Complex Data Ext on the Station screen. Used with 7500 and World Class BRI Data Modules. Does not appear on S87XX Series IP-PNC. Valid entries are valid values that conform to your dial plan. After you complete the field on the Station screen, the two extensions are associated as two parts of a one-number complex, which is the extension of the telephone.
Multimedia	Used with the 7500 and World Class BRI Data Modules. Appears only if, on the System Parameters Customer-Options (Optional Features) screen, the MM field is y. You can select this option to make this data module part of a multimedia complex.
Name	Displays the name of the user associated with the data module. The name is optional and can be blank. It can contain up to 27 alphanumeric characters. **Note:** Avaya BRI stations support ASCII characters only. BRI stations do not support non-ASCII characters, such as Eurofont or Kanafont. Therefore, if you use non-ASCII characters in any Communication Manager Name field, such characters do not display correctly on a BRI station.
Network uses 1's for Broadcast Addresses	Indicates that a broadcast address is used to send the same message to all systems or clients on a local area network. Used with Ethernet data modules.
Node Name	Appears when the Data Module type is ppp. Used with Ethernet (not on S87XX Series IP-PNC) and Point-to-Point data modules.
PDATA Port	Used to relate the physical PDATA port to which the mode 3 portion of the system port is connected. You need to enter a seven-digit alphanumeric port location to which the data module is connected. This entry must be

Field	Description
	assigned to a port on a PDATA Line Board. Used with System Port Data Modules. The valid entries are: • **01** to **22**: First and second characters are the cabinet numbers • **01** to **64**: First and second characters are the cabinet numbers (S87XX Series IP-PNC) • **A** to **E**: Third character is the carrier • **01** to **20**: Fourth and fifth characters are the slot numbers in the carrier • **01** to **12**: Sixth and seventh characters are the circuit numbers
Physical Channel	The Physical Channel number is referred to on associated system forms as the Interface Link number. Used with Netcon and Processor Interface Data Modules. The valid entries are: • **01** to **08**: For Processor Interface Data Modules, enter the 2-digit circuit number of the Processor Interface port. A multi-carrier cabinet system supports the use of two Processor Interface circuit packs, the first circuit pack (mounted in Control Carrier A) supports physical channels or links 01through 04; the second (mounted in Control Carrier A) supports physical channels or links 05 through 08. A single-carrier cabinet system supports one Processor Interface circuit pack and physical channels or links 01 through 04 only. • **01** to **04**: For DEFINITY CSI configurations. For Netcon Data Modules, enter a netcon data channel.
Remote Loop-Around Test	Indicates whether data module supports a loop-back test at the EIA interface. Appears when the Data Module Type field is set to `pdm` or `tdm`. Used with Processor/Trunk Data Modules. In general, Avaya equipment supports this test but it is not required by Level 2 Digital Communications Protocol. To abort a request for this test, you may clear this check box.

Field	Description
Secondary Data Module	Indicates that this PDM is the secondary data module used for Dual I-channel AUDIX networking. Appears only when the Type field is pdm. Used with Processor/Trunk Data Modules. The primary data module must be administered before the secondary data module can be added. If the Port field entry isx, then do not select the Secondary Data Module option.
Subnet Mask	Displays a 32-bit binary number that divides the network ID and the host ID in an IP address. Used with Point-to-Point data modules (for S87XX Series IP-PNC).
Tenant Number	Determines the music source for callers on hold. Valid entries range from **0** through **100**.

Board: Displays the five-character announcement circuit pack number that identifies the physical circuit pack to which the announcement module is connected. You can enter x in this field to indicate that there is no hardware associated with this port assignment. Used with Announcement Data Modules.

The five-character announcement board number consists of:

Characters	Meaning	Value
1 to **2**	Cabinet Number	**1** to **64** (S87XX Series IP-PNC)
3	Carrier	**A** to **E**
4 to **5**	Slot Number or X	**0** to **20**

Port: Specifies a port location to which the data module is connected. Used with 7500, Data Line, Ethernet, Processor/Trunk, PPP, System Port, and World Class BRI Data Modules.

Note:

You can enter x in the Port field to indicate that there is no hardware associated with the port assignment, also known as Administration Without Hardware (AWOH). These stations are referred to as phantom stations. If this data module is designated as a secondary data module, that is secondary data module is set to y, you cannot enter x in this field. You cannot change the port of a primary data module to x if a secondary data module is administered.

Characters	Meaning	Value
1 to **2**	Cabinet Number	**1** to **64** (S87XX Series IP-PNC)

Characters	Meaning	Value
3	Carrier	**A** to **E**
4 to **5**	Slot Number	**0** to **20**
6 to **7**	Circuit Number	• **01** to **31** (S87XX Series IP-PNC (tdm, pdm) configurations) • **01** to **16** (ppp for S87XX Series IP-PNC) • **01** to **08** (system-port for S87XX Series IP-PNC) • **17/33** (Ethernet on S87XX Series IP-PNC)

Data Module Type: Displays the type of data module.

Valid Entry	Usage
7500	Assigns a 7500 Data Module. The 7500 data module supports automatic TEI, B-channel, maintenance and management messaging, and SPID initialization capabilities. BRI endpoints, both voice and/or data, are assigned to either the ISDN-BRI - 4-wire S/T-NT Interface circuit pack or the ISDN-BRI - 2-wire U circuit pack. Each can support up to 12 ports. Since BRI provides multipoint capability, more than one ISDN endpoint (voice or data) can be administered on one port. For BRI, multipoint administration allows for telephones having SPID initialization capabilities, and can only be allowed if no endpoint administered on the same port is a fixed tie endpoint and no station on the same port has B-channel data capability. Currently, multipoint is restricted to two endpoints per port.
announcement	Assigns an announcement data module. The announcement data module is built-in to the integrated announcement circuit pack and is administered using the Announcement Data Module screen. This data module allows the system to save and restore the recorded announcements file between the announcement circuit pack and the system memory.

data-line	Assigns a Data Line Data Module. The Data Line Data Module (DLDM) screen assigns ports on the Data Line circuit pack (DLC) that allows EIA 232C devices to connect to the system. The DLC, with a companion Asynchronous Data Unit (ADU), provides a less expensive data interface to the system than other asynchronous DCP data modules. The DLC supports asynchronous transmissions at speeds of Low and 300, 1200, 2400, 4800, 9600, and 19200 bps over 2-pair (full-duplex) lines. These lines can have different lengths, depending on the transmission speed and wire gauge. The DLC has 8 ports. The connection from the port to the EIA device is direct, meaning that no multiplexing is involved. A single port of the DLC is equivalent in functionality to a data module and a digital line port. The DLC appears as a data module to the Digital Terminal Equipment (DTE) and as a digital line port to the server running Communication Manager. The DLC connects the following EIA 232C equipment to the system: • Printers • Non-Intelligent Data Terminals • Intelligent Terminals, Personal Computers • Host Computers • Information Systems Network (ISN), RS-232C Local Area Networks (LANs), or other data switches
ethernet	Specifies the name associated with an endpoint. The name you enter displays on called telephones that have display capabilities. In some messaging applications, such as Communication Manager Messaging, you can enter the user name (last name first) and their extension to identify the telephone. The name you enter is also used for the integrated directory.
ni-bri	Assigns an NI-BRI Data Module.
pdm	Assigns a DCE interface for Processor/Trunk Data Modules. These screens assign Modular Processor Data Modules (MPDMs) and Modular Trunk Data Modules (MTDMs).

	One screen is required for assigning MPDMs (700D), 7400B, 7400D or 8400B Data Module, and another screen for MTDMs (700B, 700C, 700E, 7400A). One screen must be completed for each MPDM, 7400B, 7400D, 8400B or MTDM. The MPDM, 7400B, or 8400B Data Module provides a Data Communications Equipment (DCE) interface for connection to equipment such as data terminals, CDR output devices, on-premises administration terminal, Message Server, Property Management System (PMS), AUDIX, and host computers. It also provides a Digital Communications Protocol(DCP) interface to the digital switch. (DCE is the equipment on the network side of a communications link that provides all the functions required to make the binary serial data from the source or transmitter compatible with the communications channel.) The MTDM provides an Electronic Industries Association (EIA) Data Terminal Equipment (DTE) interface for connection to off-premises private line trunk facilities or a switched telecommunications network and a DCP interface for connection to the digital switch. (DTE is the equipment comprising the endpoints in a connection over a data circuit. For example, in a connection between a data terminal and a host computer, the terminal, the host, and their associated modems or data modules make up the DTE.) The MTDM or 7400A Data Module also can serve as part of a conversion resource for Combined Modem Pooling.
ppp	Assigns a Point-to-Point Protocol data module. The PPP Data Module screen assigns a synchronous TCP/IP port on the Control Lan (C-Lan) circuit pack. These ports are tailored to provide TCP/IP connections for use over telephone lines. See *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504, for more information on Point-to-Point data modules.
system-port	Assigns a System Port Data Module.
tdm	Assigns a DTE interface for Processor/Trunk Data Modules. See the pdm entry above.

wcbri	Assigns a World Class BRI Data Module.

Button	Description
Commit	Performs the action you initiate.
Schedule	Performs the action at the specified time.
Reset	Clears the action and resets the fields.
Clear	Clears all entries.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Class of service

Class Of Service

Class Of Service (COS) allows you to administer permissions for call processing features that require dial code or feature button access. COS determines the features that can be activated by or on behalf of endpoints. Using System Manager you can view and modify the Class Of Service data.

Editing Class Of Service data

Procedure

1. On the System Manager Web Console, click **Elements** > **Messaging**.
2. In the left navigation pane, click **System** > **Class of Service**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the Class Of Service that you want to edit.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields and click **Commit** to save the changes.

Related topics:

Class of Service field descriptions on page 604

Viewing Class Of Service data

Procedure

1. On the System Manager Web Console, click **Elements** > **Messaging**.
2. In the left navigation pane, click **System** > **Class of Service**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the Class Of Service you want to view.
6. Click **View** to view the Class Of Service data.

Related topics:

Class of Service field descriptions on page 604

Filtering the Class Of Service list

Procedure

1. On the System Manager Web Console, click **Elements** > **Messaging**.
2. In the left navigation pane, click **System** > **Class of Service**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Click **Filter: Enable** in the Class Of Service List.
6. Filter the list according to one or multiple columns.
7. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

   Note:

   The table displays only those options that match the filter criteria.

Class of Service field descriptions

Name	Description
System	Specifies the name of the Communication Manager associated with the Class of Service.
Number	Specifies the Class of Service number.

General options

Name	Description
Ad-hoc video conferencing	Enables Ad-hoc Video Conferencing, so that up to six users can participate in a video conference call.
Automatic Callback	Allows users to request Automatic Callback.
Automatic Exclusion	Allows a user to activate automatically Exclusion when they go off hook on an endpoint that has an assigned Exclusion button.
Buttonless Auto Exclusion	Allows bridged appearances to operate in the exclusion mode regardless of the existence of an administered exclusion button. Currently this feature is only administrable on a per-endpoint basis by administering a feature exclusion button. This feature relaxes the requirement to use a feature button.
Call Forwarding Busy / DA	Allows users to forward calls to any extension when the dialed extension is busy or does not answer.
Call Forwarding Enhanced	Allows users to designate different preferred destinations for forwarding calls that originate from internal and external callers.
Call Forwarding All Calls	Allows users to forward all calls to any extension.
Client Room	Allows users to access Check-In, Check-Out, Room Change/Swap, and Maid status functions. In addition, Client Room is required at consoles or telephones that are to receive message waiting notification. You can administer class of service for Client

Name	Description
	Room only when you have Hospitality Services and a Property Management System interface.
Conference Tones	This feature provides the conference tone as long as three or more calls are in a conference call. If you enable these tones for countries other than Italy, Belgium, United Kingdom, or Australia, the tones will be equivalent to no tone (silence) unless the tone is independently administered or customized on the Tone Generation screen.
Console Permissions	Allows multi-appearance telephone users to control the same features that the attendant controls. You might assign this permission to front-desk personnel in a hotel or motel, or to a call center supervisor. With console permission, a user can: • Activate Automatic Wakeup for another extension • Activate and deactivate controlled restrictions for another extension or group of extensions • Activate and deactivate Do Not Disturb for another extension or group of extensions • Activate Call Forwarding for another extension • Add and remove agent skills • Record integrated announcements
Contact Closure Activation	Allows a user to open and close a contact closure relay.
Data Privacy	Isolates a data call from call waiting or other interruptions.
MOC Control	Provides the option to assign administrative control on Microsoft Office Communicator (MOC) for either of the 0-15 entries on COS or COS Group objects. By default, this check box is clear.
Extended Forwarding All	Allows a user to administer call forwarding (for all calls) from a remote location.

Name	Description
Extended Forwarding Busy / DA	Allows this user to administer call forwarding (when the dialed extension is busy or does not answer) from a remote location.
Intra-Switch CDR	Administers extensions for which Intra-Switch CDR is enabled.
Masking CPN / Name Override	Allows users to override the MCSNIC capability (that is, masking the display of calling party information and replacing it with a hard-coded, system-wide text string, Info Restricted).
Off-Hook Alert	To enable this option, either the Hospitality (Basic) or Emergency Access to Attendant field must be enabled in your license file. When enabled, these fields display as y on the System- Parameters Customer-Options screen.
Personal Station Access (PSA)	Allows users to associate a telephone to their extension with their programmed services, using a feature access code. This field must be set to n for virtual telephones. This field must be set to y at a user's home endpoint in order for that user to use the Enterprise Mobility User (EMU) feature at other endpoints.
Priority Calling	Allows users to dial a feature access code to originate a priority call. Such calls ring differently and override send all calls, if active.
Priority IP Video	Allows priority video calling, where video calls have an increased likelihood of receiving bandwidth and can also be allocated a larger maximum bandwidth per call.
QSIG Call Offer Originations	Allows users to invoke QSIG Call Offer services.
Restrict Call Fwd-Off Net	Restricts users from forwarding calls to the public network. For security reasons, this should be enabled for all classes of service except the ones you use for very special circumstances.
Trk-To-Trk Tranfer Override	Users with this COS override any system and/or COR-to-COR calling party restrictions that would otherwise prohibit the trunk-to-

Name	Description
	trunk transfer operation for users with this COS.
VIP Caller	Enables automatic priority calling when assigned to the originator of a call. A call from a VIP phone is always a priority call without the use of a feature button or FAC.

Button	Description
Commit	Saves the changes you make.
Reset	Undoes the changes you made.
Edit	Takes you to the Edit Class of Service data page.
Done	Performs the action you initiate.
Cancel	Cancels the current action and takes you to the previous page.

Authorization Code

Authorization Code

Use authorization code to control the calling privileges of system users. Authorization codes extend control of calling privileges and enhance security for remote access callers. You can use authorization codes to:

- Override a facilities restriction level (FRL) that is assigned to an originating station or trunk
- Restrict individual incoming tie trunks and remote access trunks from accessing outgoing trunks
- Track Call Detail Recording (CDR) calls for cost allocation
- Provide additional security control

Authorization Code List

Authorization Code List displays all the authorization codes under the Communication Manager you select. You can apply filters and sort each column in the Authorization Code List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Authorization Code	Displays the authorization code, which is a combination of 4 to 13 digits.
Class of Restriction	Displays the associated Class Of Restriction.
System	Specifies the name of the Communication Manager associated with the authorization code.

Viewing Authorization Code

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Authorization Code**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Authorization Code List, select the authorization code you want to view.
6. Click **View**.

Related topics:

Authorization Code field descriptions on page 609

Editing Authorization Code

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Authorization Code**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Authorization Code List, select the authorization code you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Authorization Code** page.

8. Click **Commit** to save the changes.

Related topics:

Authorization Code field descriptions on page 609

Authorization Code field descriptions

Field	Description
Authorization Code	Displays a combination of 4 to 13 digits. The number of digits must agree with the number assigned to the Authorization Code Length field on the Feature-Related System Parameters screen. To enhance system security, choose Authorization Codes of 13 random digits.
COR	Displays the Class Of Restriction. Valid entry ranges from **0** to **95**. When a user dials the associated authorization code, this is the COR that the telephone or other facility will assume for that call.

Button	Description
Commit	Performs the action you initiate.
Schedule	Performs the action at the specified time.
Reset	Clears the action and resets the fields.
Clear	Clears all entries.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Class of Service Group

Class Of Service Group

With Class Of Service Group, you can view the list of up to 100 Class Of Service (COS) groups on the screen. You can also change the configuration of individual COS group properties and edit up to 15 COS options within a group.

Class Of Service Group List

Class Of Service Group List displays the groups of Class Of Service under the Communication Manager you select. You can apply filters and sort each of the columns in the Class Of Service Group List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Group Number	Displays the number of the Class Of Service group. The group number ranges from 1 to 100.
Group Name	Displays the name of the Class Of Service group.
System	Specifies the name of the Communication Manager associated with the Class Of Service Group.

Viewing Class Of Service Group

You can view the list of up to 100 Class of Service (COS) groups on this screen.

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Class of Service Group**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.

5. From the Class Of Service Group List, select the group number for which you want to view the data.
6. Click **View**.

Related topics:

Class Of Service Group field descriptions on page 611

Editing Class Of Service Group

You can change the configuration of individual Class Of Service (COS) group properties and edit up to 15 COS options within a group on this screen.

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Class of Service Group**.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Class Of Service Group List, select the group number for which you want to edit the data.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Class Of Service Group Data** page.
8. Click **Commit** to save the changes.

Related topics:

Class Of Service Group field descriptions on page 611

Class Of Service Group field descriptions

Name	Description
System	Specifies the name of the Communication Manager associated with the Class Of Service.
Group Number	Specifies the Class Of Service number. The group number can range from **1** to **100**. This field appears when, on the System

Name	Description
	Parameters Customer-Options (Optional Features) screen, the **Tenant Partitioning** field is set to y.
Group Name	Specifies the name of the Class Of Service Group. This field appears when, on the System Parameters Customer-Options (Optional Features) screen, the **Tenant Partitioning** field is set to y.
Ad-hoc video conferencing	Enables the ad-hoc video conference capability. Six users can participate in a video conference call.
Automatic Callback	Allows users to request Automatic Callback.
Automatic Exclusion	Allows a user to activate automatically Exclusion when they go off hook on an endpoint that has an assigned Exclusion button.
Buttonless Auto Exclusion	Allows bridged appearances to operate in the exclusion mode regardless of the existence of an administered exclusion button. Currently this feature is only administrable on a per-endpoint basis by administering a feature exclusion button. This feature relaxes the requirement to use a feature button.
Call Forwarding Busy / DA	Allows users to forward calls to any extension when the dialed extension is busy or does not answer.
Call Forwarding Enhanced	Allows users to designate different preferred destinations for forwarding calls that originate from internal and external callers.
Call Forwarding All Calls	Allows users to forward all calls to any extension.
Client Room	Allows users to access Check-In, Check-Out, Room Change/ Swap, and Maid status functions. In addition, Client Room is required at consoles or telephones that are to receive message waiting notification. You can administer COS for Client Room only when you have Hospitality Services and a Property Management System interface.
Conference Tones	This feature provides the conference tone as long as three or more calls are in a

Name	Description
	conference call. If you enable these tones for countries other than Italy, Belgium, United Kingdom, or Australia, the tones will be equivalent to no tone (silence) unless the tone is independently administered or customized on the Tone Generation screen.
Console Permissions	Allows multi-appearance telephone users to control the same features that the attendant controls. You might assign this permission to front-desk personnel in a hotel or motel, or to a call center supervisor. With console permission, a user can: • Activate Automatic Wakeup for another extension • Activate and deactivate controlled restrictions for another extension or group of extensions • Activate and deactivate Do Not Disturb for another extension or group of extensions • Activate Call Forwarding for another extension • Add and remove agent skills • Record integrated announcements
Contact Closure Activation	Allows a user to open and close a contact closure relay.
Data Privacy	Isolates a data call from call waiting or other interruptions.
Extended Forwarding All	Allows a user to administer call forwarding for all calls from a remote location.
Extended Forwarding Busy / DA	Allows this user to administer call forwarding when the dialed extension is busy or does not answer from a remote location.
Intra-Switch CDR	Administers extensions for which Intra-Switch CDR is enabled.
Masking CPN / Name Override	Allows users to override the MCSNIC capability, that is, masking the display of calling party information and replacing it with a hard-coded, system-wide text string, Info Restricted.
Off-Hook Alert	To enable this option, either the Hospitality (Basic) or Emergency Access to Attendant

Name	Description
	field must be enabled in your license file. When enabled, these fields display as **y** on the System- Parameters Customer-Options screen.
Personal Station Access (PSA)	Allows users to associate a telephone to their extension with their programmed services, using a feature access code. This field must be set to n for virtual telephones. This field must be set to y at a user's home endpoint in order for that user to use the Enterprise Mobility User (EMU) feature at other endpoints.
Priority Calling	Allows users to dial a feature access code to originate a priority call. Such calls ring differently and override Send All Calls, if active.
Priority IP Video	Allows priority video calling, where video calls have an increased likelihood of receiving bandwidth and can also be allocated a larger maximum bandwidth per call.
QSIG Call Offer Originations	Allows users to invoke QSIG Call Offer services.
Restrict Call Fwd- Off Net	Restricts users from forwarding calls to the public network. For security reasons, this should be enabled for all COS except the ones you use for very special circumstances.
Trk-To-Trk Tranfer Override	Users with this COS override any system and/or COR-to-COR calling party restrictions that would otherwise prohibit the trunk-to-trunk transfer operation for users with this COS.
VIP Caller	Enables automatic priority calling when assigned to the originator of a call. A call from a VIP phone is always a priority call without the use of a feature button or FAC.

Button	Description
Commit	Performs the action you initiate.
Schedule	Performs the action at the specified time.
Reset	Clears the action and resets the fields.

Button	Description
Clear	Clears all entries.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Uniform Dial Plan Groups

Uniform Dial Plan Group

A Uniform Dial Plan Group is a set of Communication Manager systems that use the Uniform Dialing Plan (UDP) feature. You can use the Uniform Dial Plan Groups capability in System Manager to create, view, modify, and delete uniform dial plan (UDP) groups.

Adding a Uniform Dial Plan Group

About this task

Use this page to create a new UDP Group. While creating a new UDP Group, make sure that the Communication Manager systems you select share common extension ranges.

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. Click **System** > **Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, click **New**.
4. On the Add UDP Group page, enter the name for the UDP Group you want to create in the **Group Name** field.
5. Select the **Auto Update All** check box if you want the UDP tables of every Communication Manager system that you add to this group to be updated automatically.
6. Select the **Create local UDP table entry** check box if you want to create a local entry automatically in the UDP table of the Communication Manager system when you add an endpoint to it.
7. Enter the required information in the fields under the **Group Members** and **Group Ranges** tabs.

8. Click **Commit**.
9. On the System Manager console, click **Groups & Roles** > **Groups** to verify that the system added the group with the same name and resources.

Related topics:

Add UDP Groups field descriptions on page 617

Editing a Uniform Dial Plan Group

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. Click **System** > **Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, select the UDP Group that you want to modify from the UDP Group List.
4. Click **Edit**.
5. On the Edit UDP Groups page, modify the required fields.
6. Click **Commit**.

Related topics:

Add UDP Groups field descriptions on page 617

Viewing a Uniform Dial Plan Group

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. Click **System** > **Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, select the UDP Group that you want to view from the UDP Group List.
4. Click **View**. The system displays the **View UDP Group** page.

Related topics:

Add UDP Groups field descriptions on page 617

Deleting a Uniform Dial Plan Group

Procedure

1. On the System Manager Web Console, click **Elements** > **Communication Manager**.
2. Click **System** > **Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, select the UDP Group that you want to delete from the UDP Group List.
4. Click Delete.

Related topics:

Add UDP Groups field descriptions on page 617

Add UDP Groups field descriptions

Name	Description
Group Name	Enter a name for the UDP group you want to create.
Auto Update All	Select this check box if you want the UDP tables of every Communication Manager you add to this group to be updated automatically.
Create local UDP table entry	Select this check box if you want to create a local entry automatically in the UDP table of the Communication Manager system when you add an endpoint to it.

Group Members

Name	Description
CM Systems	Displays a list of Communication Manager systems from which you can select the Communication Manager you want to add to the new UDP Group. A UDP Group must contain between 2 and 10 systems.
Add	Click this link to add one or more Communication Manager systems that you want to add to the new UDP Group.

Name	Description
Element Name	Displays the name of the Communication Manager system you selected to add to the UDP group. This field is view only.
Software Version	Displays the version of the Communication Manager system you selected to add to the UDP group. This field is view only.
Remove	Click this link to remove the Communication Manager systems you selected from the **CM Systems** list.

Group Ranges

Name	Description
System Dial Plan	Displays a list of common range of extensions available on the Communication Manager systems you selected in the Group Members tab.
From	Enter the starting range of extension number.
To	Enter the closing range of extension number.
Add	Click this link to add the specified range of extension numbers.

Group Range Configuration

Name	Description
Range	Displays the range of extension numbers.
UDP Type	Enter the initials of the call-processing server network that the system uses to analyze the converted number. Valid entries are **aar**, **ars**, and **ext**.
Delete Digits	Enter the number of digits that the software deletes before the software routes a call. Valid entries are digits **0** through **3**.
Node/Location#	Enter the extension number portability (ENP) node number. Valid entries are from **1** to **999**.

Button	Description
Commit	Performs the action you initiate.
Clear	Clears all entries.

Button	Description
Cancel	Cancels your current action and takes you to the previous page.

Managing inventory

Managing application instances

Managing application instances

Inventory maintains a repository that records elements deployed in System Manager, including their runtime relationships. An element in the inventory refers to a single or clustered instance of a managed application. Inventory provides a mechanism for creating, modifying, searching, and deleting elements or application instances and the access point information from the repository. Inventory retrieves information about elements or application instances that are added or deleted from the repository.

Inventory integrates the adopting products with System Manager common console. Through Inventory, a link appears in the Application menu for each type of application instance that System Manager or the adopting products add. Inventory provides Web service APIs that the adopting applications can use for managing the elements.

Through Inventory you can:

- Create or modify application instances
- Delete elements or application instances
- Assign and remove entries for applications
- Issue a certificate to an application instance
- Replace an existing certificate
- Import bulk elements

Inventory supports the creation and updation of application systems by importing data from an XML file. You can import elements only through the graphical user interface.

Inventory supports the following configuration options for each import operation:

- Abort on First Error: The system aborts the import operation if any exception occurs.
- Continue processing other records: The system does not abort the import operation even if any exception occurs, and the import operation will continue.

Also, Inventory supports the following granularity for an import operation:

- Replace: Reimports all the data for the application system you import. This is essentially the ability to replace an existing application system and its related data with a new one.
- Merge: Merges an existing application system data with the import data from an input XML file.
- Skip: Skips the import action. As an administrator, you reimport the elements to recover from failures. If you re-import the same file to recover from failures, RTS does not over-write any record that you have successfully added. Inventory continues to process other records from the file.

Creating a new application instance

Before you begin

You have a Trust Management type entry in the **Access point** section for the application instance.

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select an application type on the Manage Elements page.
4. Click **New**.
5. On the New Entities Instance page, select the application type from the **Type** drop-down field.
6. On the **New *application type* Instance** page, complete the required fields under **Application** and **Attributes** tabs.
7. Click **Commit**.

   When you add an application entity through Runtime Topology Service (RTS), it in turn starts a synchronization job in the background to bring all the relevant data from the application instances to the Communication System Management database. To check the status of this synchronization job on the System Manager console, go to **System Manager Data** > **Scheduler** or in the log files on the Communication System Management server.

   The following information applies if you are creating an instance of messaging:

   - The FQDN or IP address details in the **Node** field for a messaging instance should correspond to that of Messaging Storage Server (MSS) and not Messaging Application Server (MAS).
   - You have to add the System Manager server details in the Trusted Server list on the Messaging box on the Messaging Administration/ Trusted Servers

screen, before adding the Messaging box in the System Manager applications.

- The login credentials between the Messaging box trusted servers screen and the Session Manager application, entity, or attributes for a Messaging type of application have to match.
- The **Trusted Server Name** field on the Trusted Server page is mapped to the **Login** field in the Attributes section. Similarly the **Password** field on the Trusted Server page is mapped to the **Password** field in the Attributes section.
- You should set the **LDAP Access Allowed** field on the Trusted Server page to **Yes** to allow LDAP access to this Messaging box from the trusted server that you add.

Viewing details of an application instance

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click an application type.
4. Select an application instance and click **View**.
   The system displays the View Application Instance page with the details of the selected application instance.

Modifying an application instance

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Click an application type on the Manage Elements page.
4. Perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. On the Edit Application Instance page, modify the required fields.

6. Click **Commit** to save the changes.

Deleting an application instance

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click an application type.
4. Select the application instance you want to delete.
5. Click **Delete**.
6. On the Delete Application Confirmation page, click **Delete**.

Importing application instances

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **More Actions** > **Import**.
4. Complete the Import Applications page, and click **Import**.

Assigning applications to an application instance

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, perform one of the following steps:
   - Select an application instance and click **Edit**.
   - If you want to assign applications to an existing application instance in the view mode, select an instance and click **View** > **Edit**.
4. Click **Assign Applications** in the Assign Applications section.

5. On the Assign Applications page, select applications and click **Assign**.

Removing assigned applications

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, perform one of the following steps:
   - If you want to remove assigned applications from an existing application instance, click an instance and then click **Edit**.
   - If you want to remove assigned applications from an existing application instance, click an instance and click **View** > **Edit**.
4. Select the applications you want to remove and click **Unassign Applications** in the Assign Applications section.

Creating a new port

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, perform one of the following steps:
   - Click **New**.
   - If you want to configure a port for an existing application instance, click an instance and then click **Edit** or click **View** > **Edit**.
4. Click **New** in the Port section.
5. Enter the information about the port in the following mandatory fields: **Name**, **Protocol**, and **Port**.
6. Click **Save**.

Result

The table in the Port Details section displays the new port.

Modifying port information

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, perform one of the following steps:
   - If you want to configure a port for an existing application instance, click an instance and then click **Edit**.
   - If you want to configure a port for an existing application instance, click an instance and click **View** > **Edit**.
4. Click **Edit** in the **Port** section.
5. Modify the port information in the following fields: **Name**, **Protocol**, **Port**, and **Description**.
6. Click **Save** to save the changes to the database.

Deleting a port

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select the application instance and click **Edit** or click **View** > **Edit**.
4. In the Port section, select the port you want to delete and click **Delete**.
   The system deletes the port you selected from the table in the Port section.

Creating an access point

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, perform one of the following steps:
   - Click **New**.

- If you want to create an access point for an existing application instance, click an instance and then click **Edit** or click **View** > **Edit**.

4. In the Access Point section, click **New** .
5. Enter the information about the access point in the following mandatory fields: **Name**, **Access Point Type**, **Protocol**, **Host**, **Port**, **URI**, and **Order**.
6. Click **Save**.

Modifying an access point

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an existing application instance and click **Edit** or click **View** > **Edit**.
4. In the **Access Point** section, select the access point you want to modify and click **Edit**.
5. Modify the access point information in the following fields: **Name**, **Access Point Type**, **Protocol**, **Host**, **Port**, **URI**, and **Order**.
6. Click **Save**.

Deleting an access point

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an existing instance and click **Edit** or click **View** > **Edit**.
4. In the Access Point section, select the access point you want to delete and click **Delete**.

Note:

You cannot delete an access point that is of type Trust Management.

Manage Elements field descriptions

Use this page to view the create, edit, view, and delete instances of the application.

Name	Description
Name	Displays the name of the application instance.
Node	Displays the node on which the application runs.
Type	Displays the type of the application to which the instance belongs. You can view this field only if you access the Manage Elements page through the **Inventory** menu.
Version	Displays the version of the application instance. You can view this field only if you access the Manage Elements page from the **Inventory** menu.
Description	Displays a brief description about the application instance.

Button	Description
View	Opens the View Other Applications Instance page. Use this page to view the details of the selected application instance.
Edit	Opens the Edit Other Applications Instance page. Use this page to modify the information of the instance.
New	Opens the New Other Applications Instance page. Use this page to create a new application instance.
Delete	Opens the Delete Other Applications Instance Confirmation page. Use this page to delete a selected application instance.
More Actions > **Configure Trusted Certificates**	Opens the Trusted Certificates page. Use this page to view, add and delete the trusted certificates for the application instance.
More Actions > **Configure Identity Certificates**	Opens the Identity Certificates page. Use this page to view and replace the identity certificates for the application instance.

Button	Description
More Actions > **Import**	Opens the Import Applications page. Use this page to bulk import application data from a valid xml file.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. **Filter: Enable** is a toggle button.
Filter: Disable	Hides the column filter fields. **Filter: Disable** is a toggle button.
Filter: Apply	Filters application instances based on the filter criteria.
Select: All	Selects all the application instances in the table.
Select: None	Clears the selection for the users that you have selected.
Refresh	Refreshes the application instance information in the table.

Application Details field descriptions

Use this page to add and edit an application instance.

Application

Name	Description
Name	Displays the name of the application instance.
Type	Displays the type of the application to which the application instance belongs.
Description	Displays a brief description about the application instance.
Node	Displays the node on which you run the application instance. **Note:** The system displays the **Node** field when you select **Other** from the **Node** field.

Port

Name	Description
Name	Displays the name of the port.
Port	Displays the port on which the application instance is running.
Protocol	Displays the protocol associated with the corresponding port.
Description	Displays a brief description about the port.

Button	Description
New	Displays fields in the Port section that you can use to add a port.
Edit	Displays fields in the Port section with port information. You can modify the port details in the port mode.
Delete	Deletes the selected configured port.
Save	Saves the port details. **Note:** The section displays the **Save** button only when you click **Add** or **Edit** in the **Port** section.
Cancel	Cancels the operation of creating or editing an access point and hides the fields that you use to enter or modify the port information. **Note:** The section displays the **Cancel** button only when you click **Add** or **Edit** in the **Port** section.

Access Point

Name	Description
Name	Displays the name of the access point.
Access Point Type	Displays the type of the access point. The options are: • **EMURL**. Use this option to create a URL type access point. • **WS**. Use this option to create a Webservice access point.

Name	Description
	• **GUI**. Use this option to create a GUI access point. • **Other**
Protocol	Displays the protocol that the application instance supports to communicate with other communication devices.
Host	Displays the name of the host on which the application instance is running.
Port	Displays the port on which the application instance is running.
Order	Displays the order in which you gain access to access points.

Button	Description
New	Displays fields in the Access Point section that you can use to add port details.
Edit	Displays fields in the Access Point section that allows you to modify the selected port details.
Delete	Deletes the selected access point.

These fields appear when you click **Add** or **Edit** in the **Access Point** section.

Name	Description
Name	Displays the name of the access point.
Access Point Type	Displays the type of the access point. The options are: • **EMURL**. Use this option to create a URL type access point . • **WS**. Use this option to create a Webservice access point. • **GUI**. Use this option to create any GUI access point. • **Other**
Protocol	Displays the protocol for communicating with the application instance.
Host	Displays the name of the host on which the application instance is running.

Name	Description
Port	Displays the port on which the application instance is running.
Order	Displays the order in which you gain access to access points.

Button	Description
Save	Saves the access point details. **Note:** This button is visible only when you click **Add** and **Edit** in the **Access Point** section.
Cancel	Cancels the operation of creating or editing an access point and hides the fields that you use to enter or modify the access point information. **Note:** This button is available only when you click **Add** and **Edit** in the **Access Point** section.

Attributes

Use this section to configure attributes for the selected application. The system displays the **Attributes** section only if the **Type** field in the **Application** section defines attributes through EP metadata.

Name	Description
Login	Login name you use for connecting to the application instance. For details, see Configuring Communication Manager user profile settings on page 456. **Note:** • craft, craft2, dadmin, inads, init, rasaccess, sroot, and tsc are the restricted logins when you configure a Communication Manager system. • Do not use the **Login** field to connect to: - Communication Manager from any other application.

Name	Description
	- The Communication Manager SAT terminal using Command Line Interface (CLI).
Password	Password which authenticates the SSH or Telnet login name on the application instance. If you gain access using Access Security Gateway (ASG), you do not require to fill this field.
Is SSH Connection	Select this check box to use SSH for connecting to the application instance. By default, the system selects the check box. If you clear the check box, the connection with the application instance is made using Telnet.
Port	The port on which the service provided by the application instance is running. The default SSH port is 5022.
Alternate IP Address	Alternate IP address of the application instance. For duplex servers, the alternate IP address is the IP address of the standby server.
RSA SSH Fingerprint (Primary IP)	The RSA SSH key of the Communication Manager server. For Duplex servers, RSA SSH Key is the key of the active server.
RSA SSH Fingerprint (Alternate IP)	The DSA SSH key of the Communication Manager server used only for duplex servers. The DSA SSH key of the standby server.
Is ASG Enabled	Select this check box to enable ASG. **Note:** If you select the **Is ASG enabled** check box, you must enter the ASG key. You do not need the password
ASG Key	The ASG key used to authenticate the ASG login. You do not have to enter any value in this field if non-ASG login is used.
Location	Displays the location of the application instance.
Enable Notifications	Provides a real-time notification whenever an administration change occurs in the Communication Manager. For example, when you add or delete an extension from

Name	Description
	Communication Manager outside System Manager. Select this checkbox to enable the CM Notify sync feature for this Communication Manager. Deselect this checkbox to disable the CM Notify sync feature for this Communication Manager. After you enable this feature and the System Manager IP address is registered on the Communication Manager, certain administrative changes that are done on the Communication Manager would be sent to System Manager asynchronously. **Note:** You need Communication Manager 6.2 or above for this feature to work.

The following fields provides information about attributes related to messaging.

Name	Description
Login	Displays the name as given in the **Trusted Server Name** field of the Trusted Servers page on the Messaging Box for this server.
Password	Password for the login name as given in the **Password** field of the Trusted Servers page on the Messaging Box for this server.
Confirm Password	Retype the password for confirmation.
Messaging Type	Displays the type of the Messaging box. The following are the types of messaging: • **MM**. For Modular Messaging systems • **CMM**. For Communication Manager Messaging systems • **AURAMESSAGING**. For Avaya Aura® Messaging systems
Version	Displays the version of the Messaging Box. Supported versions are 5.0 and above.
Secured LDAP Connection	Select this check box to use secure LDAP connection. If you clear the check box, the system uses LDAP connection.
Port	Displays the port on which the LDAP or secure LDAP service provided by the application instance is running. For LDAP the

Name	Description
	port is 389 and for secure LDAP the port is 636.
Location	Displays the location of the application instance.

The following fields provides information about attributes related to B5800 Branch Gateway device.

Name	Description
Is B5800 for Linux	Specifies whether the system type is B5800 for Linux.
Service Login	Specifies the login name through which you can access a B5800 Branch Gateway device.
Service Password	Specifies the password for accessing the B5800 Branch Gateway device.
Confirm Service Password	Retype the Service Password in this field for confirmation.
Device Version	Specifies the version of the B5800 Branch Gateway device.

SNMP Attributes

You set some basic parameters for specific devices or a range of devices in the SNMP Attributes section. You can choose either SNMP protocol V1 or V3. Based on your selection of SNMP protocol, you can then set certain basic SNMP parameters.

Name	Description
Version	Specifies the SNMP protocol type.
Read Community	Displays the read community of the device. Only applicable for SNMP protocol V1.
Write Community	Displays the write community of the device. Only applicable for SNMP protocol V1.
Retries	Displays the number of times an application polls a device without receiving a response before timing out.
Timeout	Displays the number of milliseconds an application polls a device without receiving a response before timing out.
Device Type	Specifies the type of the device.

Assign Applications

Name	Description
Name	Displays the name of the application instance.
Type	Displays the type of application.
Description	Displays a brief description about the application instance.

Button	Description
Assign Applications	Opens the Assign Applications page. Use the page to assign an application instance to another application instance.
Unassign Applications	Removes an assigned application.

Button	Description
Commit	Creates or modifies an instance by saving the instance information to the database. **Note:** This button is visible only after you click **New** and **Edit** on the Application Management page.
Cancel	Closes the page without saving the information and takes you back to the Application Management page.

Delete Application Confirmation field descriptions

Use this page to delete the selected application instance.

Name	Description
Name	Displays the name of the application instance.
Node	Displays the node on which the application is running.
Registration	Displays the registration status of the application instance. The values are: • **True**: Indicates a registered instance. • **False**: Indicates an unregistered instance

Name	Description
Description	Displays a brief description about the instance.

Button	Description
Delete	Deletes the selected application instance.
Cancel	Closes the Delete Application Confirmation page.

Assign Applications field descriptions

Name	Description
Select check box	Provides the option to select application instances.
Name	Displays the name of the application instance.
Type	Displays the type of the application.
Description	Displays a brief description about the application.

Button	Description
Assign	Assigns the selected application instance to another application instance.
Cancel	Cancels the assignment operation and takes you back to the Application Details page.

Import Applications field descriptions

Use this page to bulk import applications data from a valid XML file.

File Selection

Name	Description
Select File	Displays the path and name of the XML file from which you want to import the applications data.

Button	Description
Choose File	Opens a dialog box that you can use to select the file from which you want to import the applications data.

Configuration

Name	Description
Select Error Configuration	The options are: • **Abort on First Error**: If you select this option, system aborts importing the applications data when the import application operation encounters the first error in the import file containing the applications data. • **Continue Processing other records**: If you select this option, the system imports the data of next application if the data of previous application failed to import.
If a matching record already exists	The options are: • **Skip**: Skips a matching record that already exists in the system during an import operation. • **Replace**: Re-imports or replaces all the data for an application. This is essentially the ability to replace an application along with the other data related to the application. • **Merge**: Imports the application data at an even greater degree of granularity. Using this option you can simultaneously perform both the add and update operation of applications data. • **Delete**: Deletes the applications along with their data from the database that match the records in the input XML file.

Schedule

Name	Description
Schedule Job	The options for configuring the schedule of the job: • **Run immediately**: Use this option if you want to run the import job immediately. • **Schedule later**: Use this option to run the job at the specified date and time.
Date	Date when you want to run the import applications job. The date format is mm: dd:yyyy. You can use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.
Time	Time of running the import applications job. The time format is hh:mm:ss and 12 (AM or PM) or 24 hour format. This field is available when you select the **Schedule later** option for scheduling a job.
Time Zone	Time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Button	Description
Import	Imports or schedules the import operation based on the option you selected.

Import List

Name	Description
Select check box	Provides the option to select a job.
Start Time	Displays the time and date of scheduling the job
Status	Displays the current status of the job. The following are the different status of the job: 1. PENDING EXECUTION: The job is in queue. 2. RUNNING: The job execution is in progress. 3. SUCCESSFUL: The job execution is completed.

Name	Description
	4. INTERRUPTED: The job execution is cancelled. 5. PARTIAL FAILURE: The job execution has partially failed. 6. FAILED: The job execution has failed.
Scheduled Job	Displays a link to the Scheduler user interface. You can cancel the job from the Scheduler user interface too.
% Complete	Displays the job completion status in percentage.
Application Records	Displays the total user records in the input file.
Failed Records	Displays the number of user records in the input file that failed to import.

Button	Description
View Job	Shows the details of the selected job.
Cancel Job	Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.
Delete Job	Deletes the selected job.
Refresh	Refreshes the job information in the table.
Show	Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select **All** to view all the jobs on a single page.
Select: All	Selects all the jobs in the table.
Select: None	Clears the check box selections.
Cancel	Takes you back to the **User Management** page.

Import Status field descriptions

The Import Status page displays the detailed status of the selected import job.

Status Summary

Name	Description
Start	Displays the start date and time of the job.
End	Displays the end date and time of the job.
File	Displays the name of the file that is used to import the application records.
Total Records	Displays the total number of application records in the input file.
Successful Records	Displays the total number of applications records that are successfully imported.
Failed Records	Displays the total number of application records that failed to import.
Complete	Displays the percentage completion of the import.

Status Details

Name	Description
Line Number	Displays the line number in the file where the error occurred.
loginName	Displays the login name through which job was executed.
Error Message	Displays a brief description about the error message

Button	Description
Done	Takes you back to the Import Applications page.

Upgrade Management

Overview of Upgrade Management

Using Upgrade Management, you can get the latest software and upgrade Avaya devices. Using Upgrade Management, the system also checks the software version currently in use with regards to the latest versions available from Avaya and recommends updates when a newer version is available.

You can also download a new release from the Avaya PLDS and keep it in the software file library for upgrading the device software.

Downloading a file

About this task

Download Manager helps you to download software releases from the Avaya PLDS or SFAP.

SFAP is used for legacy devices like Communication Manager and Media Gateways. For this release only B5800 Branch Gateways are supported whose software is available in the Avaya PLDS.

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Download Manager**.
3. On the File Download Manager page, select a **Library** to where you want to download the software.
4. On the File Download Manager page, select a **Protocol** through which you want to upload the downloaded software to the Software Library from System Manager when the library is on an external server.

   Note:

   System Manager is a local library. All the protocols defined for this Software Library in the Software Library page are available for your selection.
5. On the File Download Manage page, select a software or a firmware file from the tree.
6. Do one of the following:
   - Click **Now** to download the software immediately.
   - click **Later** to schedule the download at a specified time.
7. Click **Download**.

   The system displays the End User License Agreement page.
8. Click **Accept** to download the software.

   To view the status of the download, click **Services** > **Scheduler** on the System Manager console.

   To view the progress of the download, refresh the download manager tree table.

Note:

For B5800 upgrades, you should download the file to a remote HTTP software library. You can schedule an upgrade job only for a software library configured with an http url.

The B5800 executable files are downloaded to the local System Manager repository, and are available in the `$ABG_HOME/tools` folder.

Managing software

Overview of managing software

The Manage Software feature enables you to analyze the current software on the device and recommend the available version for the device. Using the Manage Software feature, you can download the software and upgrade the devices. You can also collect the inventory or the components of a device in System Manager through the **Get inventory** button in the **Manage Software** section.

Getting inventory

Before you begin

You should enable SNMP for the B5800 Branch Gateway devices to be discovered for upgrades. You should also set the corresponding SNMPv1 communities for the devices in System Manager through **Inventory** > **Manage Elements**.

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Manage Software**.
3. On the Manage Software page, click **Get Inventory**.
4. Do one of the following:
   - Click **Now** to collect the inventory or the components of the device.
   - Click **Schedule** to get the inventory at a later time.

Analyze software

The analyze software operation finds the latest release for a device and displays the same in the **Available Software** column. The analyze operation changes the icon in the **State** column after comparing the current software version of the device against the latest version that is available. The following icons are displayed in the State column:

- Blue - represents a non-upgradable device. You cannot download software for a device with a blue icon.
- Red - software is not available in the file library for download. You should download the newer version of the software and then perform the upgrade.
- Yellow - software is available and ready for upgrade. You can schedule the upgrade anytime for this device.

The analyze operation also finds the software version a customer is entitled to. This is based on the user settings in **Upgrade Manager**.

Analyzing the software

Before you begin

Getting inventory

Configuring user settings

About this task

Using the analyze feature, you can identify whether a new software is available for the inventory you collected, and if you are entitled to download the software.

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Manage Software**.
3. On the Manage Software page, click **More Actions**.
4. Click **Analyze Now** to analyze if there is any new software available or click **Schedule** to perform the operation at a specified time.

   The system displays the state of the devices in the **State** column as icons.

   - Red: Indicates that the newer version of the software is available and the upgrade required for the device and the software file is not downloaded to System Manager Software File Library.
   - Yellow: Upgrade required for the device (newer version of s/w is available) and the s/w file is downloaded to SMGR s/w file library. i.e its Ready for Upgrade and a upgrade job can be scheduled on the device.
   - Blue: The component is not a upgradable component and only listed as part of inventory.
   - Green: the device is in the upgraded state. i.e. no newer version of the s/w is available.
   - Grey: the devices are not been analyzed yet.

Downloading the software

Before you begin

Analyze software

Create software library

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Manage Software**.
3. On the Manage Software page, select a device and then click **Download**.

   The system takes you to the Download Manager page where you can download a file for a device or devices. When the system displays the download manager page, the required files are selected as per the device selection by the user. The system displays devices with icons in the **State** column. You can download a newer version of the software for a device with a red icon.

Upgrading the device

Before you begin

Getting inventory

Analyzing the software.

Downloading the software.

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Manage Software**.
3. On the Manage Software page select a device, and click **Upgrade**.

Note:

The **Upgrade** button is enabled only if the state of a device is yellow.

Upgrade configuration

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Manage Software**.
3. On the Manage Software page, select a device and then click **Upgrade**.

   The system displays the Device Upgrade configuration page.
4. On the Device Upgrade configuration page, select a **Library** from the drop-down list.

5. Select a version from the **Release** column. You can configure a specific version other than the recommended version by selecting an option of your choice from the drop-down list.
6. Do one of the following:
   - Click **Now** to upgrade the device.
   - Click **Schedule** to upgrade the device at a specified time.

Software Library

Software Library

Software Library is used to store the downloaded software and firmware. Devices fetch these software and firmware from the library. This prevents multiple downloads of the same software of firmware for different devices requiring the same file.

Using **Software Library** you can create, modify, view, and delete the software library having the upgrade files.

Creating a software library

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Software Library**.
3. Click **New**.
4. Complete the Add Software Library page.
5. Click **Commit**.
   Click **Clear** to reset the page.

Related topics:

Setting up the external server to work as a remote software library for B5800 upgrades on page 651

Editing a software library

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Software Library**.
3. Select the software library whose details you want to edit.
4. Click **Edit**.

5. Edit the required fields in the Edit Software Library page, and click **Commit**.

Viewing a software library

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Software Library**.
3. Select the software library whose details you want to view.
4. Click **View**.

   The system displays the details of the software library you selected through the View Software Library page.

Deleting a software library

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Software Library**.
3. Select the software library you want to delete.
4. Click **Delete**.
5. On the confirmation page click **Delete**.

Library Server Details

You can use Library Server Details (L) to configure basic parameters of the software library.

Name

Specifies the name of the software library.

IP Address

Specifies the IP address of the software library.

Description

Specifies the description of the software library.

Server Path

Specifies the path to the software library where all the downloaded files are stored.

Default Library

Specifies whether the library is a default library.

Remote Library

Specifies whether the library is a remote library.

Default Protocol

The default protocol for the software library that you can associate with the software library name. The available selections are:

- **FTP**: Select FTP as the default protocol for the software library.
- **SCP**: Select SCP as the default protocol for the software library.
- **SFTP**: Select SFTP as the default protocol for the software library.
- **HTTPS**: Select HTTPS as the default protocol for the software library.

Note:

Based on your default protocol selection, when you select the library name on the File Download Manager page, the system selects the associated protocol.

HTTP/HTTPS URL

Enables you to specify the software library URL.

Note:

When you select HTTPS for the default protocol, this field becomes mandatory.

FTP Configuration (F)

You can use FTP Configuration (F) to configure FTP protocol details for the software library.

Note:

When you select **FTP** for the default protocol on the Library Serve Details (L) page, then these parameters are mandatory.

Enable FTP

Select to enable the FTP configuration.

FTP User Name

Specifies the user name for the FTP configuration.

FTP Password

Specifies the password for the FTP configuration.

Retype FTP Password

Select to retype the FTP password.

SCP Configuration (S)

You can use SCP Configuration (S) to configure SCP protocol details for the software library.

Note:

When you select **SCP** for the default protocol on the Library Serve Details (L) page, then these parameters are mandatory.

Enable SCP

Select to enable the SCP configuration.

SCP User Name

Specifies the user name for the SCP configuration.

SCP Password

Specifies the password for the SCP configuration.

Retype SCP Password

Select to retype the SCP password.

SFTP Configuration (T)

You can use SFTP Configuration (T) to configure SFTP protocol details for the software library.

Note:

When you select **SFTP** for the default protocol on the Library Serve Details (L) page, then these parameters are mandatory.

Enable SFTP

Select to enable the SFTP configuration.

SFTP User Name

Specifies the user name for the SFTP configuration.

SFTP Password

Specifies the password for the SFTP configuration.

Retype SFTP Password

Select to retype the SFTP password.

Enable HTTP/HTTPS

Select to enable to HTTP/HTTPS configuration.

HTTP/HTTPS URL

Enables you to specify the software library URL.

Note:

When you select HTTPS for the default protocol, this field becomes mandatory.

User Name

User name for the HTTP/HTTPS configuration.

Password

The password for the HTTP/HTTPS configuration.

Retype Password

Retype the HTTP/HTTPS password in this field.

HTTP/HTTPS Configuration

You can use HTTP/HTTPS Configuration to configure HTTP/HTTPS protocol details for the software library.

Adding a file to the software library

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Software Library**.
3. Click **More Actions** > **Manage Files**.
4. On the Software Library Files page, click **New**.
5. Click **New**.
6. Complete the Add File page, and click **Commit**.
   Click **Clear** to clear the fields.

Note:

You can add files of 25000000 bytes or less.

Editing a file in the software library

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Software Library**.
3. Click **More Actions** > **Manage Files**.
4. On the Software Library Files page select the file whose details you want to edit.
5. Click **Edit**.
6. Edit the required fields and click **Commit**.

Viewing a file in the software library

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Software Library**.
3. Click **More Actions** > **Manage Files**.
4. On the Software Library Files page select the file you want to view.
5. Click **View**.
   You can view the details of the file in the View File page.

Deleting a file from the software library

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Upgrade Management** > **Software Library**.
3. Click **More Actions** > **Manage Files**.
4. On the Software Library Files page select the file or files you want to delete.
5. Click **Delete**.
6. On the confirmation page click **Delete**.

Manage software library files field descriptions

Name	Description
Software Library	The software library where the file is created.
Product Family	The product family which the file belongs to. Under a product family number of devices are listed.
Device Type	The device type for which the software library file can be used for upgrade. For example, for a B5800 Branch Gateway, B5800 and B5800 for Linux are the device types.
Software Type	The type of software file which includes firmware, images.
File	The software file that you upload from your local directory to the selected library.
File Version	The software file version that you upload.
Hardware Compatibility	Hardware compatibility for the file you upload. For B5800 Branch Gateway this field can be null.

Button	Description
Commit	Adds the file to the software library. Saves the changes you have made in the Edit File page.
Edit	Allows you to edit the file details for the file you selected.
Done	The system displays the Software Library Files page after you view the file details through the **View** button.

Button	Description
Clear	Clears your entry and resets the fields.
Cancel	Cancels your current action. The system displays the previous page.

Remote software library for upgrading B5800 element firmware

Remote Software Library for B5800 upgrades

For the B5800 firmware upgrade files, an external server is required to act as a remote software library. This server hosts the firmware upgrade files through HTTP. The external server should have an FTP, or an SCP, or an SFTP server to download the firmware files from the PLDS Web site.

Note:

HTTPS protocol, used to extract the firmware file from the external server, is currently not supported by System Manager.

Downloading the firmware files from PLDS to the B5800 elements through System Manager

1. Download the B5800 firmware from PLDS to the System Manager cache using the credentials provided in **User Settings** in System Manager.
2. Upload the firmware to the external server from the System Manager cache using the FTP or SCP or SFTP protocol and the configuration information in the software library.
3. After the file is on the external server, B5800 elements use this file during upgrade using HTTP protocol.

Note:

Steps 1 and 2 happen simultaneously. The file download to System Manager is transparent.

System requirements for the external server

Component	Requirement	Recommendation
Operating System	Any standalone or virtualized Windows or Linux Distribution.	
Hard Drive	20GB free space	There should be enough free space on the hard drive to store the firmware files.
Memory	2GB	As required by the operating system and the supported protocol services.

Component	Requirement	Recommendation
Protocols (for the B5800 elements to download files from the external server)	HTTP server	Any supported HTTP server installation. **Note:** HTTPS is currently not supported by System Manager.
Protocols (for downloading the firmware upgrade files to the external server from PLDS site via System Manager)	An FTP or an SCP or an SFTP server (running on default ports)	Use SFTP or SCP for secure file transfer.

Setting up the external server to work as a remote software library for B5800 upgrades

Procedure

1. Install the operating system.
2. Install any supported HTTP server.
3. Install any one of the supported servers (FTP or SFTP or SCP).
4. Configure users for the FTP or SFTP or SCP access. These users should have read, write, and delete permissions for the directories configured to serve as the storage location for the upgrade files.
5. Configure the HTTP server such that the location where the upgrade files are downloaded is accessible using an HTTP URL. This URL is used to configure the external server as a software library on System Manager. This HTTP URL is used by the B5800 elements to pull the firmware files during upgrade. Therefore this URL must be reachable to the B5800 elements.

Related topics:

Creating a software library on page 644

User Settings

You can use the User Settings page to configure the location from where System Manager displays information on the latest software, firmware releases. Additionally, using the User Settings page, you can also specify the PLDS, Proxy, and SFAP credentials for the software download.

Use Avaya support site

To find information on the software releases from the Avaya support site.

Other Website

Defines the Web site location from where the latest software is available. This is an alternate option to the Avaya support site.

Note:

Ensure that the latest `versions.xml` file and software files are available at this location.

SSO User

To provide the user name to be used as single sign on for Avaya PLDS.

SSO Password

Specifies the single sign on password.

Confirm SSO Password

Retype the SSO password in this field.

Use Proxy

Select this check box to enable the use of a proxy server for PLDS.

Host

Specifies the host name of the proxy.

Port

Specifies the port of the proxy.

Use SFAP

Select the check box to use the Avaya's Software and Firmware Access Policy (SFAP) for downloading software and firmware for Avaya devices.

User Name

Specifies the user name for SFAP, that is, the customer ID.

Password

Password for SFAP.

Confirm Password

Retype the SFAP password in this field.

User BP Link ID

Specifies the user business partner (BP) link ID.

BP Link ID

To provide your business partner (BP) link ID.

Retrieve SoldTos

Retrieves all the available SoldTos.

SoldTos

Select a SoldTo from the list of available SoldTos.

Collected Inventory

Collected Inventory

The **Collected Inventory** tab displays a list of all the inventory components or items that are collected. After the inventory collection is complete, the system lists the collected devices. You can either choose the **Tree** View or the **List** View for viewing all the discovered devices.

Collected Inventory list

The Collected Inventory list displays all the inventory components or items that are discovered. This list also displays some of the properties of the devices. You can sort this list according to any of the columns in the list.

There are two default views of the Collected Inventory list: List View and Tree View.

- The List View lists every entity that is collected. In this view, each entity appears as a separate row.
- The Tree View displays the inventory items in groups. The inventory items are grouped by the device type.

Viewing the Collected Inventory list

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. Click **Collected Inventory** in the left navigation pane.
   The system displays the **Collected Inventory** list, which gives the details of the inventory collected.

   Note:

   This is a read-only list.
3. Click an IP address in the inventory list to view more information about the device.

   When you click an IP address in the list, the system displays a pop up which contains more information about the inventory items for that IP address. This information varies according to the device you choose.

Related topics:

Collected Inventory list field description on page 655

Filtering the Inventory list

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. Click **Collected Inventory** in the left navigation pane.
3. Click **Filter: Enable** in the Collected Inventory list.
4. Filter the list according to one or multiple columns.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

Note:

The table displays only those options that match the filter criteria.

Using Advanced Search in Collected Inventory

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. Click **Collected Inventory** in the left navigation pane.
3. Click **Advanced Search**.
4. In the Criteria section, do the following:
   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter the search value in the third field.

   If you want to add a search condition, click the plus sign (**+**) and repeat the sub steps listed in step 3.

   If you want to delete a search condition, click the minus sign (**-**) . This button is available if there is more than one search condition.

Collected Inventory list field description

Name	Description
Name	Name of the device.
IP	IP address of the device.
Family	Specifies the device family type. Possible values include Communication Manager, Media Gateway and Switches; Application and Element Managers.
Type	Specifies the type of the device.
Module	Module ID of the device.
Description	Specifies the description of the device.
Software/Firmware Version	Software release of the device.
Hardware Version	Hardware version of the device.
Location	Location of the device.
Serial Number	Serial number of the hardware.

Inventory Management

Overview of Inventory Management

You can use the Inventory Management feature to configure System Manager to discover specific devices within the network. This feature also lets you manage the SNMP access parameters used for the inventory collection process.

Inventory Management detects or discovers your network, including subnets and nodes. Inventory Management exclusively uses Simple Network Management Protocol (SNMP) to discover your network.

Inventory Management in System Manager includes:

- Configuring the SNMP access parameters, Communication Manager access parameters, and subnets.
- Collecting the inventory.

SNMP Access list

You can use the SNMP Access list to configure the basic SNMP parameters for specific devices or for a range of devices. **Inventory Management** recognizes SNMP V1 and V3 protocols. For both these protocols, access parameters also include timeout and retry values.

Name	Description
Type	Specifies the SNMP protocol type. Possible values are: • **V1** • **V3**
Read Community	The read community of the device. Only applicable for SNMP V1 protocol.
Write Community	The write community of the device. Only applicable for SNMP V1 protocol.
User	Specifies the user name as defined in the application. Applicable for SNMP V3 protocol only.
Auth Type	Specifies the authentication protocol that authenticates the source of traffic from SNMP V3 protocol users. Possible values are: • **MD5 (default)** • **SHA** Authorization type is applicable only for SNMP V3 protocol.
Priv Type	The encryption policy for SNMP V3 users. Possible values are: • **DES**: Use DES encryption for SNMP-based communication. • **AES**: Use AES encryption for SNMP-based communication • **No Privacy**: Do not encrypt traffic for this user Privacy type is applicable only for SNMP V3 users.
Timeout (ms)	Specifies the number of milliseconds discovery waits for the response from the device being polled.

Name	Description
Retries	Specifies the number of times discovery polls a device without receiving a response before timing out.
Description	Describes the SNMP Access profile.

Setting the order in the SNMP Access list

About this task

You can set the order in which you want to list the SNMP Access profiles in the SNMP Access list. While polling a device, the SNMP Access profiles are used according to this list.

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Select the SNMP Access profile you want to move up or move down.
4. Do one of the following:
   - Click **Move Up** if you want to set the SNMP Access profile one step ahead in the list.
   - Click **Move Down** if you want to set the SNMP Access profile one step down in the list.

Related topics:

SNMP Access list on page 656

Adding an SNMP Access profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Click **New** from the **SNMP Access (A)** tab.
4. Select the SNMP protocol type from the **Type** field.
5. Complete the **Add SNMP Access Configuration** page and click **Commit**.

Related topics:

SNMP Access field descriptions on page 658

Editing an SNMP Access profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Select the SNMP Access profile you want to edit from the **SNMP Access (A)** tab..
4. Click **Edit**.
5. Edit the required fields on the **Edit SNMP Access Configuration** page.
6. Click **Commit** to save the changes.

Related topics:

SNMP Access field descriptions on page 658

Deleting an SNMP Access profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Select the SNMP Access profiles you want to delete from the **SNMP Access (A)** tab.
4. Click **Delete**.
5. Confirm to delete the SNMP Access profiles.

SNMP Access field descriptions

For SNMP protocol V3

Name	Description
Type	Specifies the SNMP protocol type. Value can be either V1 or V3.

Name	Description
User	User name as defined in the application.
Authentication Type	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. Possible values are: • **MD5 (default)** • **SHA** Authorization Type is applicable only for SNMP V3 protocol.
Authentication Password	The password used to authenticate the user. Passwords must consist of at least eight characters.
Confirm Authentication Password	You must re-type the SNMP V3 protocol authentication password for confirmation.
Privacy Type	The encryption policy for an SNMP V3 user. Possible values are: • **DES**- Use DES encryption for SNMP based communication. • **AES**- Use AES encryption for SNMP based communication. • **No Privacy** - Do not encrypt traffic for this user. Privacy Type is only required for an SNMP V3 user.
Privacy Password	The password used to enable DES or AES encryption, if you select DES as the Privacy Type. DES Passwords must consist of at least eight characters.
Confirm Privacy Password	You must re-type the privacy password in this field for confirmation.
Timeout (ms)	The number of milliseconds discovery waits for the response from the device being polled.
Retries	The number of times discovery polls a device without receiving a response before timing out.

For SNMP protocol V1

Field	Description
Type	Specifies the SNMP protocol type. Value can be either V1 or V3.
Read Community	The read community of the device. Only applicable for SNMP V1 protocol.
Write Community	The write community of the device. Only applicable for SNMP V1 protocol.
Timeout (ms)	The number of milliseconds discovery waits for the response from the device being polled.
Retries	The number of times discovery polls a device without receiving a response before timing out.

Button	Description
Commit	Adds or edits the SNMP Access profile (whichever applicable).
Reset	Undoes your action.
Cancel	Takes you to the previous page.

Subnet(s) (S) list

The Subnet(s) (S) List contains the list of subnets that are manually added.

Name	Description
Subnet IP	IP address of the subnet.
Subnet Mask	Specifies the IP subnet mask.
Use SNMP V3	Specifies whether you want to only use SNMP V3 protocol. Select the check box to only use SNMP V3 protocol.

Button	Description
Commit	Adds or edits the subnet.
Reset	Undoes all the entries.
Cancel	Cancels your current action and takes you to the previous page.

Adding a subnet

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Click the **Subnet(s) (S)** tab.
4. Click **New**.
5. Complete the Add Subnet Configuration page and click **Commit**.

Related topics:

Subnet(s) (S) list on page 660

Editing a subnet

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Click the **Subnet(s) (S)** tab.
4. Select the subnet you want to edit.
5. Click **Edit**.
6. Edit the required fields on the **Edit Subnet Configuration** page.
7. Click **Commit** to save the changes.

Related topics:

Subnet(s) (S) list on page 660

Deleting a subnet

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Click the **Subnet(s) (S)** tab.

4. Select the subnets you want to delete.
5. Click **Delete**.
6. Confirm to delete the subnets.

CM Access list

The CM Access list specifies the Communication Manager login parameters to connect to the Communication Manager servers in your network.

Name	Description
IP address	IP address of the Communication Manager.
Port	Login port of the Communication Manager.
Login	Login name as configured on the Communication Manager server.
Use ASG Key	Indicates the use of ASG encryption.
Use SSH	Indicates the use of SSH protocol.
Global profile	Specifies the default parameters that can be used to configure a Communication Manager server in the Entities application in System Manager.

Filtering Subnet(s) (S) and CM Access (C) lists

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Click **Filter: Enable** in the Subnet(s) (S) list or the CM Access 9C) list.
4. Filter the subnets or the CM access profiles according to one or multiple columns.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

   Note:

   The table displays only those options that match the filter criteria.

Adding a Communication Manager Access profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Click the **CM Access (C)** tab.
4. On the Configuration page, click **New**.
5. Complete the Add CM Access details page and click **Commit**.

Related topics:

CM Access profile field descriptions on page 664

Editing a Communication Manager Access profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Click the **CM Access (C)** tab.
4. Select the Communication Manager Access profile you want to edit.
5. Click **Edit**.
6. Edit the required fields on the Edit CM Access details page.
7. Click **Commit** to save the changes.

Related topics:

CM Access profile field descriptions on page 664

Deleting a Communication Manager Access profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Configuration**.
3. Click the **CM Access (C)** tab.

4. Select the Communication Manager Access profile you want to delete.
5. Click **Delete**.
6. Confirm to delete the Communication Manager Access profile.

CM Access profile field descriptions

Name	Description
IP Address	IP address of the Communication Manager.
Port	Login port of the Communication Manager.
Login	Login name as configured on the Communication Manager server.
Password	Password for logging in.
Confirm Password	Re-enter password for confirmation.
Use ASG Key	Indicates the use of ASG encryption.
ASG key	Specifies the ASG password or key for login. ASG key is a 20 character octal code.
Use SSH	Indicates the use of SSH protocol.
Global Profile	Specifies the default parameters that can be used to configure a Communication Manager server in the Entities application in System Manager. You can select this checkbox only once. This checkbox is disabled once you configure the Global Profile.

Button	Description
Commit	Adds or edits the Communication Manager Access profile.
Reset	Undoes the current action.
Cancel	Cancels the current action and takes you to the previous page.

Collect Inventory

Using the **Collect Inventory** tab in **Inventory Management**, you can configure the subnets and device types to be collected. You must select the subnet as well as the device type before starting the inventory collection process.

Collecting the inventory

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Discovery**.
3. Select the subnet and the device type from the Select Network Subnet(s) list and the Select Device Type(s) list respectively.
4. Click **Now** to start the collect inventory process.

Note:

To schedule the collect inventory process at a later time, click **Schedule**.

Note:

To restart the collect inventory process, select the **Clear previous results** check box. When you select this check box, the discovered devices are removed only from the inventory list and not from the Entities application.

Related topics:

Collect Inventory field descriptions on page 666

Filtering Network Subnet(s)

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Inventory Management** > **Discovery**.
3. Click **Filter: Enable** in the Network Subnet(s) list.
4. Filter the network subnet(s) according to one or multiple columns.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

Note:

The table displays only those options that match the filter criteria.

Collect Inventory field descriptions

Select Network Subnet(s) list

Name	Description
Subnet IP	IP address of the subnet.
Subnet Mask	Specifies the subnet mask.
Use SNMP V3	Specifies whether you want to only use SNMP V3 protocol. Select the checkbox to only use the SNMP V3 protocol.
Inventory Collection Status	Provides information about the current inventory collection status. Possible values include: • **Pending** • **In Progress** • **In Progress: preparing for inventory collection** • **In Progress: probing network elements** • **In progress: collecting inventory information** • **In progress: saving inventory information** • **Failed** • **Idle**
Last Inventory Collection Time	Latest time when the inventory collection was carried out.

Select Device Type(s) list

Name	Description
Device Type	Specifies the type of the device.
Description	Describes the device type.

Managing Serviceability Agents

Serviceability Agents

The Serviceability Agent is an enhanced version of the SAL agent for forwarding logs, harvesting logs, and for alarming. The Serviceability Agent sends SNMPv2, SNMPv3 traps and informs to the configured NMS destinations where two of the mandatory destinations are System Manager itself and the SAL gateway.

With the Serviceability Agent user interface you can:

- Remotely manage and configure SNMPv3 users
- Remotely manage and configure SNMP trap destinations
- Create, edit, view, and delete user and target profiles. You can also attach these profiles to agents or detach these profiles from agents.

Managing SNMPv3 user profiles

Creating an SNMPv3 user profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click **New**.
4. On the New User Profile page, complete the User Details section.
5. Click **Commit**.

Related topics:

SNMPv3 user profiles field descriptions on page 669

Editing an SNMPv3 user profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Select the user profile you want to edit from the Profile List.

4. Click **Edit**.
5. Edit the required fields in the Edit User Profile Page.
6. Click **Commit**.

Related topics:

SNMPv3 user profiles field descriptions on page 669

Viewing an SNMPv3 user profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click the user profile you want to view from the Profile List.
4. Click **View**.
   You can view the details, except the password, of the SNMPv3 user profile in the View User Profile Page.

Related topics:

SNMPv3 user profiles field descriptions on page 669

Deleting an SNMPv3 user profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Select the user profile or profiles you want to delete from the Profile List.
4. Click **Delete**.
5. On the User Profile Delete Confirmation page, click **Delete**.

Note:

You cannot delete a user profile that is attached to an element or a target profile.

Filtering SNMPv3 user profiles

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.

2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click **Filter: Enable** above the Profile List.
4. Apply the filter to one or multiple columns of the User Profile List.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear the filter criteria that you set in the column filters.

SNMPv3 user profiles field descriptions

Name	Description
User Name	Specifies the SNMPv3 user name. **Note:** The user name can contain the following characters: alphanumeric, period, underscore, white space, single quote, and hyphen. The user name cannot be an empty string.
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are: • MD5 (default) • SHA The default value is MD5.
Authentication Password	The password used to authenticate the user. **Note:** The password can contain any printable and non-white space characters of 8 to 255 length. The password cannot be an empty string.
Confirm Authentication Password	Retype the authentication password in this field for confirmation.
Privacy Protocol	The encryption policy for an SNMP V3 user. The possible values are: • DES: Use DES encryption for SNMP-based communication. • AES: Use AES encryption for SNMP-based communication.

Name	Description
	The default value is AES.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Confirm Privacy Password	Retype the privacy password in this field for confirmation.
Privileges	The read-write privilege that determines the operations you can perform on MIBs. The default value is **None**. Using a read-write privilege, you can perform both GET and SET operations. With a Read privilege, you can perform only the GET operation.

Button	Description
Commit	Use to create a new SNMPv3 user profile. Saves the changes after an edit operation.
Back	Cancels the action and takes you to the previous page.
Delete	Use to delete the user profiles you select.
Edit	Use to edit the user profile you select.

Managing SNMP target profiles

SNMP Target profile list

Name	Description
Name	The name of the SNMP target profile. This name should be a unique value.
Domain Type	The type of transport for the flow of messages. The default value is UDP.
IP Address	The IP address of the SNMP target profile.
Port	The port of the SNMP target profile.
SNMP Version	The version of the SNMP protocol.

Button	Description
New	To go to the New Target Details page where you can add a new SNMP target profile.

Button	Description
View	To go to the View Target Details page where you can view an existing SNMP target profile.
Edit	To go to the Edit Target Details page where you can edit an existing SNMP target profile.
Delete	To delete the existing SNMP target profiles that you select.
Filter: Enable	To filter the SNMP target profiles list by one or multiple criteria.

Filtering target profiles

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. Click **Filter: Enable** above the Profile List.
4. Apply the filter to one or multiple columns of the Target Profile List.
5. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear the filter criteria that you set in the column filters.

Creating an SNMP target profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. On the SNMP Target Profiles page, click **New**.
4. On the New Target Details page, complete the Target Details section.
5. To attach a user profile, click the **Attach/Detach User Profile** tab. This applies only if you chose the SNMPv3 protocol.
6. Click **Commit**.

Related topics:

SNMP target profile field descriptions on page 673

Viewing an SNMP target profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. From the Target Profile list, click the profile you want to view.
4. Click **View**.
   You can view the details of the target profile in the View Target Details page.

Related topics:

SNMP target profile field descriptions on page 673

Editing an SNMP target profile

About this task

Note:

You must modify the target profiles pointing to the System Manager to reflect the changed IP address in the event of an IP change on the System Manager.

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. From the Target Profile list, click the profile you want to edit.
4. Click **Edit**.
5. On the Edit Target Details page, modify the required fields.
6. Click **Commit**.

Related topics:

SNMP target profile field descriptions on page 673

Deleting an SNMP target profile

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. From the Target Profile list, click the profile or profiles you want to delete.

4. Click **Delete**.
5. On the Delete Confirmation page, click **Delete**.

Note:

You cannot delete a target profile that is attached to an element or an agent.

SNMP target profile field descriptions

Name	Description
Name	The name of the SNMP target profile.
Description	The description of the SNMP target profile.
IP Address	The IP address of the target profile.
Port	The port of the target profile.
Domain Type	The type of the message flow. The default value is UDP.
Notification Type	The notification type.
Protocol	The type of the SNMP protocol.

Button	Description
Commit	Creates the target profile in the New Target Profile page or saves the changes in the Edit Target Profile page.
Back	Cancels your action and takes you to the previous page.

Managing user and target profiles

Serviceability Agents list

Name	Description
Hostname	The host name of the server on which the serviceability agent runs.
IP Address	The IP address of the server on which the serviceability agent runs.
System Name	The system name of the server on which the serviceability agent runs.
System OID	The system OID of the server on which the serviceability agent runs.

Name	Description
Status	The enabled or disabled status of the serviceability agent. The system disables SNMPv3 and displays **Inactive** as the default status.

Activating a serviceability agent

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select an agent you want to manage.
4. Click **Activate**.

   This activates the SNMPv3 functionality in the remote serviceability agent that you selected. If the system does not activate the SNMPv3 functionality for some reason, refresh the Web page and repeat Step 3 and Step 4.

Related topics:

Managing target profiles for the selected serviceability agents on page 674
Managing SNMPv3 user profiles for the selected serviceability agents on page 675

Managing target profiles for the selected serviceability agents

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. From the Agent List, select one or multiple active agents that you want to manage.
4. Click **Manage Profiles**.
5. Click the **SNMP Target Profiles** tab.
6. Select the target profiles you want to assign from the Assignable Profiles section.
7. Click **Assign**.

   Similarly, you can unassign or remove target profiles from the Removable Profiles section by clicking **Remove**.
8. Click **Commit** to assign the profiles to the selected agent.

Note:

You can also select several serviceability agents and assign the same target profiles to all of them.

Related topics:

Activating a serviceability agent on page 674
Managing SNMPv3 user profiles for the selected serviceability agents on page 675

Managing SNMPv3 user profiles for the selected serviceability agents

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. From the Agent List, select an active agent that you want to manage.
4. Click **Manage Profiles**.
5. Click the **SNMPv3 User Profile** tab.
6. Select the user profiles you want to assign from the Assignable Profiles section.
7. Click **Assign**.

   Similarly, you can unassign or remove user profiles from the Removable Profiles section by clicking **Remove**.
8. Click **Commit** to assign the user profiles to the selected agent.

Note:

You can also select several serviceability agents and assign the same user profiles to all of them.

Related topics:

Activating a serviceability agent on page 674
Managing target profiles for the selected serviceability agents on page 674

Communication Profiles synchronization

Communication profiles synchronization

System Manager provides the account synchronization feature to synchronize profiles between CS 1000 or CallPilot communication profile and their elements. Using this feature you

can synchronize profiles in User Management with the profiles in the elements. During synchronization, the account synchronization feature uses the account data in the elements as the master data. Therefore, when a profile data is not in synchronization with the element, the account data from the element is copied to System Manager.

Synchronizing CS 1000 and CallPilot profiles

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **CS 1000 and CallPilot Synchronization**.
3. Select the element you want to synchronize.
4. Do one of the following:
   - Click **Start** to begin the synchronization.
   - Click **Stop** to stop the synchronization process. The other buttons are disabled when you click Stop.
   - Click **Clear** to clear all the synchronization displayed.
   - Click **Reload** to refresh.

Related topics:

Synchronize communication profiles field descriptions on page 677

Assigning anonymous profiles

About this task

When a synchronization process completes, the **Summary** column displays any anonymous element accounts in the element. You can assign the anonymous account to users or delete the accounts from the element.

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **CS 1000 and CallPilot Synchronization**.
3. On the Synchronize Communication Profiles page, click the anonymous profile you want to assign from the **Summary** column.
   The system displays the Anonymous Communication Profiles page with the details of each anonymous account.
4. Select one of the anonymous accounts.

5. Enter the name in the **Name (Last, First)** field.
6. Click **Assign**.
   The Anonymous Communication Profiles page refreshes with an update of the **Status** of the assigned account.

Related topics:

Anonymous Communication Profiles field descriptions on page 678

Deleting anonymous profiles

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **CS 1000 and CallPilot Synchronization**.
3. On the Synchronize Communication Profiles page, click the anonymous profile you want to delete from the **Summary** column.
   The system displays the Anonymous Communication Profiles page with the details of each anonymous account.
4. Select the anonymous account you want to delete.
5. Click **Delete**.
   The system displays a confirmation dialog box.
6. Click **OK**.

Synchronize communication profiles field descriptions

Name	Description
Element	Name of the CS 1000 or CallPilot system.
Status	Current status of the synchronization process. The following are the possible values: • Queued - The synchronization task is queued and runs automatically once other synchronization tasks have completed. • Running - The synchronization is running. This status appears once you click the **Start** button.

Name	Description
	• Stopping- The synchronization is stops if you click the **Stop** button. • Aborted - This status appears once the synchronization stops completely. • PASS - This status indicates that the synchronization is complete. • FAIL - This status indicates that the synchronization has failed. You can look into thje log files for the information on the failure.
Date	Displays the date when the synchronization started.
Summary	Displays the number of accounts processed, the number of anonymous accounts, the number of accounts added, updated and deleted. When no accounts are processed, this field displays “O account(s) processed”.

Button	Description
Start	Starts a synchronization process.
Stop	Stops a synchronization process that is in the running state.
Clear	Clears all the synchronization results that are processed.
Reload	Refreshes the synchronization status once again.

Anonymous Communication Profiles field descriptions

Name	Description
Name (Last, First)	Type the user name to whom you want to assign this communication profile.
Service Information	The service information of the CS 1000 or CallPilot system.
Target	The system customer number of the element.
Status	Displays the status of the anonymous profile. The status can be assigned or anonymous.

Button	Description
Assign	Assigns the user to the anonymous profile you select.
Delete	Deletes the anonymous profile you select after confirmation
Cancel	Cancels your assign or delete action and takes you to the previous page.

Synchronization of Data

Communication Manager, Messaging data, and B5800 Branch Gateway synchronization

Managed elements have alternative ways of administering data. To ensure uniformity in the database when a variety of tools are used, you can use the synchronization menu. You can synchronize Communication Manager, messaging data, and B5800 Branch Gateway through this menu.

Communication System

Using System Manager, you can synchronize the System Manager data with the Communication Manager system. When you add Communication Manager to the system, System Manager automatically initiates synchronization to update the System Manager database.

Initializing synchronization

Initializing synchronization allows you to synchronize data in the System Manager database with each managed Communication Manager system. When you add a Communication Manager into the system, System Manager automatically initiates an initialization task to get all the Communication Manager data that is required, and stores it in the System Manager database.

Incremental synchronization

Incremental synchronization with selected devices allows you to incrementally synchronize data in the System Manager database with each managed Communication Manager system. This synchronization updates the changed data in the database in Communication Manager since synchronization was last run.

B5800 Branch Gateway system

Using System Manager, you can synchronize the System Manager data with B5800 Branch Gateway. When you add a new B5800 Branch Gateway to System Manager automatically initiates synchronization to update the System Manager database.

Synchronizing messaging data

You can also synchronize messaging data in System Manager with the Messaging, Communication Manager Messaging, and Modular Messaging systems.

Note:

You must add a new Communication Manager or a messaging entity through Application Management before you perform synchronization.

Scheduled synchronization

You can create and schedule synchronization jobs using System Manager. You can schedule a synchronization job to run at a fixed time and repeat it periodically. System Manager provides a default incremental synchronization every 24 hours. You can modify this to your convenience.

On-demand synchronization

System Manager allows you to synchronize data with the Communication Manager on demand. Administrators can initiate this at any time. On-demand synchronization can either be initialization synchronization or an incremental synchronization.

Related topics:

Initializing Synchronization on page 681
Incremental Synchronization on page 681
Saving the Communication Manager translations on page 683

Synchronizing Communication Manager data and configuring options

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Communication System**.
3. Select the Communication Manager device you want to synchronize.
4. Below the device list, select any of the following options that you want to synchronize for the selected device:
   - **Initialize data for selected devices**: Using this option, you can synchronize data in the System Manager database with each managed Communication Manager system.

     Note:

     When you add a Communication Manager to the system, System Manager automatically initiates an initialization task to get all the Communication Manager data that is required, and stores it in the System Manager database.

- **Incremental Sync data for selected devices**. Using this option, you can synchronize incrementally with the selected devices data in the System Manager database with each managed Communication Manager system.

  Note:

  This synchronization updates the changed data in the database in Communication Manager since synchronization was last run.

- **Save Translations for selected devices**. Using this option, you can save the configuration of the selected device on the same device, Communication Manager itself.

5. To perform the synchronization now, click **Now** and to perform the synchronization at a specified time, click **Schedule**.

   Note:

   To view the status of synchronization, on the System Manager Web Console, click **Services** > **Scheduler**.

Initializing Synchronization

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Communication System**.
3. Select the Communication Managers you want to synchronize.
4. Select **Initialize data for selected devices**.
5. To initialize synchronization, click **Now** or perform one of the following tasks:
   - To perform the synchronization at a specified time, click **Schedule**.
   - To cancel the synchronization, click **Cancel**.

Incremental Synchronization

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Communication System**.
3. Select the Communication Manager systems that you want to synchronize.

4. Select **Incremental Sync data for selected devices**.
5. Click **Now** to perform the incremental synchronization or do one of the following:
   - To perform the synchronization at a specified time, click **Schedule**.
   - To cancel the synchronization, click **Cancel**.

Note:

While scheduling incremental synchronization, set the logging levels on Communication Manager using the **change logging-levels** option. In the **Log Data Values** field, select `both`.

When you add a Communication Manager system, the default incremental synchronization jobs will be scheduled 1 hour after the maintenance job starts on Communication Manager.

If the incremental synchronization of the Communication Manager data fails due to the overlapping of Communication Manager synchronization and maintenance jobs, change the default scheduled job time in the Pending Jobs page.

Synchronizing the B5800 Branch Gateway system configuration

Procedure

1. On the System Manager console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **B5800 Branch Gateway**.
3. Select the device you want to synchronize.
4. Below the device list, select any of the following options that you want to synchronize for the selected device:
   - **System Configuration**: This option enables you to get the latest system configuration of the device and update the same in System Manager.
   - **User**: This option enables you to synchronize all the users present in System Manager from the selected device.
   - **System Configuration and Users**: This option enables you to get the latest system configuration and details of all the users from the selected device and synchronize with System Manager.
5. Click **Now** to perform the synchronization now or click **Schedule** to perform the synchronization at a specified time.

Note:

To view the status of synchronization, click **Services** > **Scheduler** on the System Manager console.

Synchronizing the messaging data

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Messaging Data**.
3. Select the messaging systems you want to synchronize.
4. To perform the synchronization, click **Now** or perform one of the following tasks:
   - To perform the synchronization at a specified time, click **Schedule**.
   - To cancel the synchronization, click **Cancel**.

Saving the Communication Manager translations

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Communication System**.
3. From the list, select a Communication Manager system.
4. Select **Save Translations for selected devices**.
5. To save the System Manager administration changes in Communication Manager, click **Now**.

   To save the translations at a specified time, click **Schedule**.

Note:

After running the **Save translation job**, the system may not update the last saved translation time in the Communication Manager list. This might be because the save translation operation is slow when Communication Manager has large data or translations to save. In such conditions, the system updates the last saved translation time only on the next incremental synchronization after the save translations operation is complete on Communication Manager.

Configure options

The Uniform Dial Plan (UDP) call type works identically with the ext call type, with an exception: if the dialed digits match the call type of UDP, Communication Manager automatically checks the UDP table to see if there is a match, regardless of the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen. If there is no match, Communication Manager then checks the local server.

If the dialed digits match the call type of ext, Communication Manager checks the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen.

If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is **udp-table-first**, Communication Manager checks the UDP Table first to see if there is a match. If there is no match, Communication Manager then checks the local server.

If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is **local-extensions-first**, Communication Manager checks the local server first to see if there is a match. If there is no match, Communication Manager then checks the UDP table.

The UDP call type allows Communication Manager to recognize strings of 14 to 18 digits, which are longer than the maximum extension length of 13 digits. However, the UDP call type can be used with any length in case this provides a useful new capability to customers.

UDP in System Manager

You can select the Uniform Dial Plan option on the Synchronize CM Data and Configure Options page from **Elements** > **Communication Manager** > **System** > **Uniform Dial Plan Groups**. When you select the **Consider UDP** option, the system does not use the corresponding dial plan for the available extension range while adding an endpoint. When you do not select the **Consider UDP** option, the system uses the corresponding dial plan for the available extension range while adding an endpoint.

Managing messaging

Messaging Class Of Service

A Class Of Service (COS) is a set of messaging capabilities that you define and assign to subscribers. The Class Of Service page lists the current name and number of the different Classes Of Service. You can only view the COS names and numbers on this screen; you cannot use this screen to change the COS names or numbers.

Viewing Class Of Service

Procedure

1. On the System Manager Web Console, click **Elements** > **Messaging**.
2. Click **Class Of Service** in the left navigation pane.
3. Choose one or more messaging systems from the Messaging Systems list.
4. Click **Show List**.
5. Click the respective column heading to sort the Class Of Service by **Name** in alphabetical order or by **Class No.** in numeric order.

   This is a read-only list.

Class of Service List field descriptions

Name	Description
Class No	Specifies the number of each class of service.
Name	Specifies the name of the class of service.
Last Modified	Specifies the time and date when the class of service was last modified.
Messaging System	Specifies the type of messaging system.

Messaging

Subscriber Management

You can perform selected messaging system administration activities through System Manager. You can add, view, edit, and delete subscribers through System Manager. Apart from subscriber management, you can also administer mailboxes and modify mailbox settings for a messaging system.

System Manager supports:

- Communication Manager 5.0 and later
- Avaya Aura® Messaging 6.0 and later
- Avaya Aura® Modular Messaging 5.0 and later
- Communication Manager Messaging 5.2 (with patch having LDAP support) and later

Adding a subscriber

Procedure

1. On the System Manager Web Console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select one or more messaging systems from the list of Messaging Systems.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions**, and **Miscellaneous** sections.
7. Complete the **Add Subscriber** page and click **Commit** to add the subscriber.

Note:

If you select more than one Messaging, Modular Messaging, or Communication Manager Messaging from the list of messaging systems, and then click **New**, the system displays the Add Subscriber page with the first Messaging, Modular Messaging, or Communication Manager Messaging in context.

Related topics:

Subscribers (Messaging) field descriptions on page 689
Subscribers (CMM) field descriptions on page 694
Subscribers (MM) field descriptions on page 697

Editing a subscriber

Procedure

1. On the System Manager Web Console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.

4. Click **Show List**.
5. From the Subscriber List, choose the subscriber you want to edit.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields in the **Edit Subscriber** page.
8. Click **Commit** to save the changes.

Related topics:

Subscribers (Messaging) field descriptions on page 689
Subscribers (CMM) field descriptions on page 694
Subscribers (MM) field descriptions on page 697

Viewing a subscriber

Procedure

1. On the System Manager Web Console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Select the subscriber you want to view from the Subscriber List.
6. Click **View**.

Note:

You cannot edit any field on the View Subscriber page.

Related topics:

Subscribers (Messaging) field descriptions on page 689
Subscribers (CMM) field descriptions on page 694
Subscribers (MM) field descriptions on page 697

Deleting a subscriber

Procedure

1. On the System Manager Web Console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.

3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Select the subscriber you want to delete from the Subscriber List.
6. Click **Delete**.
   The system displays a confirmation page for deleting the subscriber.
7. Confirm to delete the subscriber or subscribers.

Note:

You cannot delete a subscriber associated with a user through mailbox management. You can delete the user associated subscribers only through User Profile Management.

Subscriber List

Subscriber List displays all the subscribers under a messaging version, such as Messaging, Communication Manager Messaging, or Modular Messaging. You can apply filters to each column in the Subscriber List. You can also sort the subscribers according to each of the column in the Subscriber List. When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Name	Specifies the name of the subscriber.
Mailbox Number	Specifies the mailbox number of the subscriber.
Email Handle	Specifies the e-mail handle of the subscriber.
Telephone Number	Specifies the telephone number of the mailbox.
Last Modified	Specifies the time and date when the subscriber details were last modified.
User	If a subscriber is associated with a user, then the system displays the name of the user in this column.
System	Specifies the messaging system of the subscriber.

Filtering subscribers

Procedure

1. On the System Manager Web Console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Click the **Filter: Enable** option in the Subscriber List.
6. Filter the subscribers according to one or multiple columns.
7. Click **Apply**.
   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

Note:

The table displays only those subscribers that match the filter criteria.

Subscribers (Messaging) field descriptions

Field	Description
Type	Specifies the messaging type of the subscriber template.
Template Name	Specifies the messaging template of a subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.

Field	Description
Mailbox Number	Displays the full mailbox number of a subscriber, including the site group and site identifiers and the short mailbox number. Subscribers use mailbox numbers to log on to their respective mailbox. For a PBX subcriber, the mailbox number ranges from three to ten digits in length. Other local subscribers use this field to address messages to the PBX subscriber. For a Multisite system subscriber, the mailbox number is up to 50 digits in length. Ensure the mailbox number is: • In the range of mailbox numbers assigned to your system • Unassigned to another local subscriber • Of a valid length on the local computer This is a mandatory field on the Add Subscriber pages for all types of messaging systems.
PBX Extension	The primary telephone extension of the subscriber. For a Multisite system subscriber, this number is up to 50 digits in length.
Class Of Service	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client

Field	Description
	applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]).
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII version of name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Subscriber Security

Field	Description
Expire Password	Specifies whether your password expires or not. You can choose one of the following: • **yes**: for password to expire • **no**: if you do not want your password to expire
Is Mailbox Locked?	Specifies whether you want your mailbox to be locked. A subscriber mailbox can become locked after two unsuccessful login attempts. You can choose one of the following: • **no**: to unlock your mailbox • **yes**: to lock your mailbox and prevent access to it

Mailbox Features

Field	Description
Personal Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.

Field	Description
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, callers can page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
VoiceMail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: use this to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to

Field	Description
	hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary Extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Miscellaneous 1	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 2	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 3	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 4	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Saves all the changes.
Edit	Allows you to edit the fields.
Reset or **Clear**	Clears all the changes.

Button	Description
Cancel	Takes you to the previous page.

Subscribers (CMM) field descriptions

Field	Description
System	Specifies the messaging system of the subscriber you want to add.
Template	Specifies the template for this subscriber. You can choose any template from the drop-down box.
Type	Specifies the messaging type of your subscriber.
Software Version	Specifies the messaging version of the subscriber.
Save as Template	Saves your current settings as a template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3 to10-digits in length, that the subscriber will use to log on to the mailbox. Other local subscribers can use the Mailbox Number to address messages to this subscriber. The Mailbox Number is: • Within the range of Mailbox Numbers assigned to your system. • Not assigned to another local subscriber. • A valid length on the local computer.
Mailbox Number	Displays the full mailbox number of a subscriber, including the site group and site identifiers and the short mailbox number. Subscribers use mailbox numbers to log on to their respective mailbox. For a PBX subcriber, the mailbox number ranges from three to ten digits in length. Other local subscribers use this field to address

Field	Description
	messages to the PBX subscriber. For a Multisite system subscriber, the mailbox number is up to 50 digits in length. Ensure the mailbox number is: • In the range of mailbox numbers assigned to your system • Unassigned to another local subscriber • Of a valid length on the local machine This is a mandatory field on the Add Subscriber pages for all types of messaging systems.
Password	The default password that a user has to use to login to his or her mailbox. The password you enter can be 1 to 15–digits in length and cannot be blank
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter `0` through `99`, or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter `0` if no message waiting indicators should be sent for this subscriber. You should enter `0` when the subscriber does not have a telephone on any switch in the network.
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain a combination of digits from 0 to 9. If an account code is not specified, the system will use the

Field	Description
	subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that the system displays before the computer name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Field	Description
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber to the messaging system.
Schedule	Adds the subscriber at the specified time.
Save as Template	Saves the settings as a template.
Reset	Clears all the changes.
Edit	Allows you to edit the fields.
Done	Completes your action and takes you to the previous page.
Cancel	Takes you to the previous page.

Subscribers (MM) field descriptions

Field	Description
System	Specifies the messaging system of the subscriber you want to add. You can choose this option from the drop-down box.
Type	Specifies the messaging type of your subscriber.
Template	Specifies the messaging template of a subscriber. You can choose an option from the drop-down box.
Software Version	Specifies the message version of the subscriber.
Save as Template	Saves your current settings as a template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
Mailbox Number	Displays the full mailbox number of a subscriber, including the site group and site identifiers and the short mailbox number. Subscribers use mailbox numbers to log on to their respective mailbox. For a PBX subcriber, the mailbox number ranges from three to ten digits in length. Other local subscribers use this field to address messages to the PBX subscriber. For a Multisite system subscriber, the mailbox number is up to 50 digits in length. Ensure the mailbox number is: • In the range of mailbox numbers assigned to your system • Unassigned to another local subscriber • Of a valid length on the local computer. This is a mandatory field on the Add Subscriber pages for all types of messaging systems.
PBX Extension	The primary telephone extension of the subscriber. For a Multisite system subscriber, this number is up to 50 digits in length.
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her

Field	Description
	mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that the system displays before the computer name and domain in the subscriber's e-mail address. The computer name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]).
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Subscriber Security

Field	Description
Expire Password	Specifies whether your password expires or not. You can choose one of the following: • **yes**: for password to expire • **no**: if you do not want your password to expire
Is Mailbox Locked?	Specifies whether you want your mailbox to be locked. A subscriber mailbox can become

Field	Description
	locked after two unsuccessful login attempts. You can choose one of the following: • **no**: to unlock your mailbox • **yes**: to lock your mailbox and prevent access to it

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.

Field	Description
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, callers can page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: use this to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for

Field	Description
	convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber to the messaging system.
Schedule	Adds the subscriber at the specified time.
Save as Template	Saves the settings as a template.
Reset	Clears all your changes.
Edit	Allows you to edit all the fields.
Done	Completes your current action and takes you to the previous page.
Cancel	Takes you to the previous page.

Chapter 6: Managing backup and restore

Backup and Restore

The backup and restore functions are executed through System Manager. With these functions, you can back up and restore configuration data for System Manager and all of the Session Manager instances. All of the configuration data for the entire system is kept centrally on System Manager. This means that individual backups of the Session Manager instances are not needed. After a restore operation, the restored configuration data is automatically propagated to the Session Manager instances.

Associated actions include configuring data retention rules for specifying how long the backup files should remain on the system, and modifying logger and appender information.

Ensure sufficient disk space is available before taking local back up.

Note:

All the backups that you schedule within an hour after a restore operation will be skipped. After an hour all the recurring jobs will be executed at the specified time. This is done so that your new backup does not overwrite the earlier backup when a restore fails.

Backup and restore operations are mutually exclusive. You can perform either a backup or a restore operation at a given time. So, a restore fails if a backup operation is already running.

Accessing the Backup and Restore service

Procedure

On the System Manager Web Console, click **Services** > **Backup and Restore**.

Result

The system displays the Backup and Restore page.

Viewing list of backup files

Procedure

On the System Manager Web Console, click **Services** > **Backup and Restore**.
The Backup and Restore page displays the list of backup files.

Related topics:

Backup and Restore field descriptions on page 709

Creating a data backup on a local server

Procedure

1. On the System Manager Web Console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In the **File name** field, enter the file path and the name of the backup file that you want to create.
5. Click **Now**.
   If the backup is successful, the Backup and Restore page displays `Backup created successfully!!`

Related topics:

Backup field descriptions on page 710

Creating a data backup on a remote server

Procedure

1. On the System Manager Web Console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.

3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Specify the remote server IP, remote server port, user name, password, and name and path of the backup file that you want to create.
   - Select the **Use Default** check box.

   Important:

   To use the **Use Default** option, ensure that you specify the remote server IP, user name, password, and name and path of the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
5. Click **Now**.
   If the backup is successful, the Backup and Restore page displays `Backup created successfully!!`

Related topics:

Backup field descriptions on page 710

Scheduling a data backup on a local server

Procedure

1. On the System Manager Web Console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local** option.
4. In the **File name** field, enter the name of the backup file that you want to create.
5. Click **Schedule**.
6. On the Schedule Backup page, specify the following details in the appropriate fields:
   - Job name
   - Date and time when the system must run the job
   - Frequency at which the system must run the job
   - Range
7. Click **Commit**.

Related topics:

Backup field descriptions on page 710
Schedule Backup field descriptions on page 711

Scheduling a data backup on a remote server

Procedure

1. On the System Manager Web Console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
   - Select the **Use Default** check box.

   Important:

   To use the **Use Default** option, ensure that you specify the remote server IP, user name, password, and name and path of the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
5. Click **Schedule**.
6. On the Schedule Backup page, specify the following details in the appropriate fields:
   - Job name
   - Date and time when the system must run the job
   - Frequency at which the system must run the job
   - Range
7. Click **Commit**.

Related topics:

Backup field descriptions on page 710
Schedule Backup field descriptions on page 711

Restoring data backup from a local server

Procedure

1. On the System Manager Web Console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Local**.
4. In the **File name** field, type the file name that you want to restore.

   If the file name does not appear in the list, specify the complete path of the file you want to restore.
5. Click **Restore**. On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no services will be available until the operation completes. So, the System Manager console will not be available for approximately 45 minutes but this time may vary based on Database size. Click on Continue to go ahead with the Restore operation or click on Cancel to abort the operation.
   ```
6. Click **Continue**.
   The system logs you out of the System Manager console and then shuts down.

Related topics:

Restore field descriptions on page 712

Restoring a backup from a remote server

Procedure

1. On the System Manager Web Console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. Perform one of the following:
   - Specify the remote server IP, remote server port, user name, password to access the remote computer and name of the file that you want to restore in the respective fields

- Select the **Use Default** check box.

Important:

To use the **Use Default** option, ensure that you specify the remote server IP, user name, password, and name and path of the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

5. Click **Restore**. On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no
   services will be available until the operation completes. So,
   the System Manager console will not be available for
   approximately 45 minutes but this time may vary based on
   Database size. Click on Continue to go ahead with the Restore
   operation or click on Cancel to abort the operation.
   ```

6. Click **Continue**.
   The system logs you out of the System Manager console and then shuts down.

Related topics:

Restore field descriptions on page 712

Performing a restore through the command line interface

About this task

You can perform a restore operation through the command line especially when the machine is in an unstable state and the system does not display the GUI.

Procedure

1. Go to `$MGMT_HOME/pem/fileRestoreCLIUtility`.
2. Modify `restorecli.properties`. Enter the build number of the machine in the **version** field.

   Ensure that `fq_backup_file_name` displays the complete path of the backup zip file.
3. Modify `fileRestoreCLIUtility.properties` so that `backup_name` points to the backup zip file.

4. From the shell, execute the **sh $MGMT_HOME/pem/fileRestoreCLIUtility/file_restore.sh<full path of fileRestoreClIUtility><0/1>** command.

   Where, *0* denotes only the file restore and *1* denotes a full restore.

5. Complete the steps on the screen to perform the restore operation successfully.

Backup and Restore field descriptions

Use this page to view the details of backup files or the files you want to restore.

Name	Description
Operation	Specifies the type of operation. The values are: • Backup • Restore
File Name	• For the backup operation, specifies the name of the backup file. • For the restore operation, specifies the name of the file you want to restore.
Path	• For the backup operation, specifies the path of the backup file. • For the restore operation, specifies the path of the file you want to restore.
Status	Indicates the status of the backup or restore operation. The values are: • SUCCESS • FAILED • PLANNED • RUNNING
Operation Time	Specifies the time of the backup or restore operation.
Operation Type	The type defines whether the backup or restore operation is a local or remote.
User	The user who has performed the operation.

Button	Description
Backup	Opens the Backup page. Use this page to back up data on a specified local or remote location.
Restore	Opens the Restore page. Use this page to restore data to a specified local or remote location.

Backup field descriptions

Use this page to backup the System Manager data on a local or a remote location. You can also use this page to schedule a backup job.

Name	Description
Type	Specifies the type of computer on which you can back up the application data. The options are: • **Local**: The system backs up the data on a local computer. • **Remote**: The system backs up the data on a remote computer.

The page displays the following fields when you choose to create a backup of System Manager data on a local computer.

Name	Description
File Name	Specifies the name of the file that identifies the backup. If you specify only the file name, System Manager creates a backup file in the home directory of the specified user. To create the backup file in a directory other than the home directory, specify a complete path including the file name.

The page displays the following fields when you choose to create a backup of System Manager data on a remote server.

Name	Description
Remote Server IP	Specifies the IP address of the remote server.
Remote Server Port	Specifies the SSH port of the remote server.

Name	Description
User Name	Specifies the user name for logging into the remote server.
Password	Password for logging on to the remote server.
File Name	Specifies the path and name of the file that identifies the backup. If you specify only the file name, System Manager creates a backup file in the default directory of the user. You can specify a different path for the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
Use Default	Select this check box to use the default configured values. To use the **Use Default** option, ensure that you specify the remote server IP, user name, password, and name and path of the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

Button	Description
Now	Backs up the data to the specified location immediately.
Schedule	Opens the Schedule Backup page. Use this page to schedule a back up.
Cancel	Closes the Backup page and takes you back to the Backup and Restore page.

Schedule Backup field descriptions

Use this page to schedule a job for backing up data by specifying the date and time.

Job Details

Name	Description
Job Name	Specifies the name of the job.

Job Frequency

Name	Description
Task Time	Specifies the date and time of running the job.
Recurrence	The settings define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field also displays the time interval of recurrence. The options are: • Execute task one time only. • Tasks are repeated.
Range	The settings define the number of recurrences or date after which the job stops to recur. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules the backup job.
Cancel	Closes the Schedule Backup page and takes you back to the Backup Restore page.

Restore field descriptions

Use this page to restore application data from a local or a remote location.

Name	Description
Type	Specifies the type of computer from which you want to restore the application data. The options are: • **Local**. The data is restored from a local machine. • **Remote**. The data is restored from a remote machine.

The page displays the following fields, when you select **Local** as **Type**.

Name	Description
File Name	Specifies the name of the backup file that you want to restore. If the system does not display the file you want to restore, specify the complete path of the backup file.
Select File Name	Lists the name of the backup file that you want to restore.

The page displays the following fields, when you select **Remote** as **Type**.

Name	Description
Remote Server IP	Specifies the IP address of the SCP server.
Remote Server Port	Specifies the SSH port of the SCP server.
User Name	Specifies the user name for logging in to the SCP server.
Password	Password for logging in to the SCP server.
File Name	Specifies the name and complete path of the backup file that you want to restore.
Use Default	Select this check box to use the default configured values. To use the **Use Default** option, ensure that you specify the remote server IP, user name, password, and name and path of the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

Button	Description
Restore	Restores the data from the specified backup file.
Cancel	Closes the Restore page and takes you back to the Backup and Restore page.

Chapter 7: Bulk Import and Export

Using System Manager, you can import and export user profiles and elements. The bulk import of data is done using an XML file that is validated against an XML schema definition. The output of a bulk export operation is an XML file.

You can perform the System Manager bulk import through the System Manager Web interface. When you initiate the bulk import function from the Web interface, System Manager schedules the import as a job. The System Manager Web interface provides the file for bulk import. You can run the job immediately or schedule an import job for a later date or time.

Important:

System Manager 6.2 does not support the bulk import and export of roles.

You can perform bulk export in System Manager through the Command Line Interface (CLI).

The System Manager bulk import and export feature supports:

- User-related data. Identity data, Communication Profile set and handles, Communication Profiles such as the endpoint data, the messaging data, and the Session Manager data
- Global settings such as Public Contact Lists, Shared Addresses, and System Presence ACLs
- Element data

The following are the key features of the bulk import:

- You can add, modify, and delete user records.
- System Manager supports a maximum of 250000 users in bulk export or import in multiple files.
- You can configure skip, replace, merge, or delete a matching record that already exists.
- To bulk import user logs for failed records, you must manually perform through the System Manager Web console.
- For bulk import of users, you can download failed records in an XML file format. The XML file must conform to the XML schema definition. You can modify and re-import the failed records.
- If you encounter problem in any record during a bulk import, you can choose the continue on error option.
- While importing users, you can perform a complete or a partial import. To add a subset of user data, you can use partial import. For example, you can replace only the Communication Profile, the user contact lists, or the user ACLs. When you import new users in the database, you must perform complete import.

Chapter 8: System Manager configuration

Managing data retention rules

Accessing the Data Retention Rules service

Procedure

1. On the System Manager Web Console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.
   The system displays the Data Retention page with the Rule list.

Result

The system displays the Data Retention page.

Data retention rules

You can configure data retention rules for specifying the time in days you want the system to retain the following records:

- Logs
- Cleared alarms
- Aged alarms

Viewing data retention rules

Procedure

1. On the System Manager Web Console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.

The system displays the Data Retention page with the Rule list.

Related topics:

Data Retention field descriptions on page 718

Modifying data retention rules

Procedure

1. On the System Manager Web Console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.
   The system displays the Data Retention page with the Rule list.
3. Select a rule from the Rule list.
4. Click **Edit**.
5. Modify the value in the **Retention Interval (Days)** field.
6. Click **Update** to save the value.

Related topics:

Data Retention field descriptions on page 718

Data Retention field descriptions

Use this page to view and edit data retention rules.

Name	Description
Option button	Provides the option to select a data retention rule.
Rule Name	Specifies the name of the rule.
Rule Description	A brief description about the data retention rule.
Retention Interval (Days)	Specifies the number of days the data is retained.

Button	Description
Edit	Modifies the selected rule.

Button	Description
Update	Updates the rule with changes made to the rule.
Cancel	Cancels the editing operation.
Apply	Applies the selected rule.

Setting service profiles for applications

Service Profile Management

Service Profile Management provides a configuration repository for System Manager services. Service Profile Management is responsible for storing configuration data for System Manager services and notifying the services of configuration changes.

You can perform the following operations using Service Profile Management:

- Store configuration data for services.
- View a profile of a service.
- Edit a profile of a service.

View global feature profiles

This topic is about the global feature profiles that Service Profile Manager maintained in System Manager.

Following is the global feature profile for System Manager:

View Profile System Manager field descriptions on page 732

Edit global feature profiles

This topic is about the global feature profiles that Service Profile Manager maintained in System Manager. You must log in as administrator to edit the global profiles.

Following is the global feature profile for System Manager:

Edit Profile System Manager field descriptions on page 733

View Profile: Agent Management field descriptions

Use this page to view the parameters and their values that are set for managing agents.

Name	Description
Alarm aging keep time	This field is not used for System Manager.
Enterprise auto download	The value in this field specifies whether to enable or disable enterprise auto downloading. The default value is false. If the value is set to true, the enterprise downloads the base rules for all registered agents.
Enterprise customer reference	The customer reference for the Enterprise. For example, Avaya. A value in this field is required only if polling to upstream enterprise is enabled.
Enterprise heartbeat interval	The time in seconds between heartbeats for Enterprise to Enterprise communication. A value in this field is required only if polling to upstream enterprise is enabled.
Enterprise heartbeat threshold	The heartbeat threshold in seconds for the Enterprise. A value in this field is required only if polling to upstream enterprise is enabled.
Enterprise platform name	The value in this field specifies a fully-qualified DataTransport address of the host Enterprise. For example: The value of this field will be "avaya.com., Enterprise-dtxjbss01", if the OrganizationFQDN value is "avaya.com." and SpiritPlatformQualifier value is "Enterprise-dtxjbss01". A value in this field is required only if polling to upstream enterprise is enabled.
Enterprise tenancy support	This field is for tenancy support of SAL. This field is not used for System Manager.
Enterprise upstream platform name	The value specifies a fully-qualified Data Transport address of the upstream enterprise. For example: The value of this field is "avaya.com., Enterprise-dtxapp06", if the Connection.AvayaTest.FQDN value is "avaya.com." and

Name	Description
	Connection.AvayaTest.PlatformQualifier value is "Enterprise-dtxapp06". A value in this field is required only if polling to upstream enterprise is enabled.
Enterprise upstream polling	The value in this field specifies whether polling upstream enterprise is enabled or not. The default value is false. A false value disables upstream Enterprise polling or Cascading Enterprise.
Inventory aging keep time	This field is not used for System Manager.
Inventory change keep time	This field is not used for System Manager.
Out Of Service delete time	This field is not used for System Manager.

Button	Description
Edit	Opens the Edit Profile: Agent Management page. Use this page to edit the parameters in the Agent Management profile.
Done	Closes the View Profile: Agent Management page.

Related topics:

View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734
View Profile: User Bulk Import Profile field descriptions on page 759

View Profile: Alarm Management field descriptions

Use this page to view the parameters and their values that are set for managing alarms generated by System Manager and its components.

Name	Description
Email from address	The value is the e-mail address of the alarm manager. For example: alarmgr@avaya.com
Email hostname	The value is the name of the SMTP e-mail host.

Name	Description
	For example, “306181anex4.global.avaya.com”
Email to addresses	The values are comma separated list of e-mail addresses to which alarms are forwarded.
Email user id	The value is the e-mail address of the user.
Federation member platform name	A fully qualified data transport address to which alarms are forwarded. For example, the value of this field will be "avaya.com., Enterprise-dtxapp06", if the Connection.AvayaTest.FQDN value is "avaya.com." and Connection.AvayaTest.PlatformQualifier value is "Enterprise-dtxapp06".
NMS forward	The value specifies whether alarms are to be forwarded to Network Management System (NMS). The default value is false. If set to true, the SAL forwards the alarms to the NMS
NMS urls	A comma separated list of NMS (Network Management System) URLS. For example, "[155.184.73.11:162]" There are no default values from SAL Enterprise and you need to update them later.
SPIRIT ui url	The URL for accessing theala SAL Web interface for viewing a specific alarm.
Trouble ticket url	The URL for accessing the Trouble Ticket Web interface. **Note:** Do not change this value.

Button	Description
Edit	Opens the Edit Profile: Alarm Management page. Use this page to edit the parameters in the Alarm Management profile.
Done	Closes the View Profile: Alarm Management page.

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Event processor field descriptions on page 726

View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734
View Profile: User Bulk Import Profile field descriptions on page 759

Configuring B5800 Branch Gateway

Procedure

1. On the System Manager console, click **Services** > **Configurations**.
2. Click **Settings** > **B5800 Branch Gateway** > **Configuration**.
3. On the View Profile: Configuration page click **Edit**.
4. Edit the table properties and general properties in the Edit Profile: Configuration page.
5. Click **Commit**.

B5800 Branch Gateway profile field descriptions

B5800 Branch Gateway table Properties

Name	Description
Maximum Records for Select All in table	Specifies the maximum number of records that is used for selection if **Select All** is used in list pages.
Maximum Records on single page of table	Specifies the maximum number of records displayed in the table.

General Properties

Name	Description
Application Prefix	The default value in this field is B5800. This application prefix appears as the prefix in the Communication System Management job names.

Button	Description
Edit	System displays the Edit

Button	Description
Done	Insert a description of what happens when this button is clicked.
Commit	Saves the changes you make on the Edit: Profile page.
Cancel	Cancels your action and takes you to the View: Profile page.

View Profile: Communication System Management Configuration field descriptions

Use this page to edit the parameters in the Communication System Management Configuration profile.

General Properties

Name	Description
Application Prefix	The default value in this field is CSM. This application prefix appears as the prefix in the Communication System Management job names.

Telephony

Name	Description
Clean-up Old Backup Announcement Files interval (Days)	The time between every clean up of the backed up announcement files. The default value is 30 days.
Incremental sync interval (Hours)	The time between every incremental synchronization. By default, the value for the **incremental_sync_interval_in_hours** field is 24.
Maximum Records for select All in table	Specifies the maximum number of records that is used for selection if **Select All** is used in list pages.
Maximum Records on single page of table	Specifies the maximum number of records displayed in the table.

Button	Description
Edit	Opens the Edit Profile:Communication System Management Configuration page.

Button	Description
	Use this page to edit the parameters in the Scheduler profile.
Done	Closes the Edit Profile:Communication System Management Configuration page.

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734
View Profile: User Bulk Import Profile field descriptions on page 759

Edit Profile: Communication System Management Configuration field descriptions

Use this page to edit the parameters in the Communication System Management Configuration profile.

General Properties

Name	Description
Application Prefix	The default value in this field is CSM. This application prefix appears as the prefix in the Communication System Management job names.

Telephony

Name	Description
Clean-up Old Backup Announcement Files interval (Days)	The time between every clean up of the backed up announcement files. The default value is 30 days.
Incremental sync interval (Hours)	The time between every incremental synchronization. By default, the value for the incremental_sync_interval_in_hours field is 24.
Maximum Records for select All in table	Specifies the maximum number of records that is used for selection if **Select All** is used in list pages.

Name	Description
Maximum Records on single page of table	Specifies the maximum number of records displayed in the table.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the Edit Profile:Communication System Management Configuration page.

Related topics:

Edit software feature profiles on page 734
Edit Profile:Logging Service field descriptions on page 743

View Profile: Event processor field descriptions

Use this page to view the parameters and their values that are set for managing events.

Name	Description
EP mechanism class name 1	This field is not used for System Manager.
EP mechanism XSD type	The value in this field specifies event processor uses a set of XML rule configuration files to describe the rules to be used to process events. The event processor uses a different processing mechanisms as indicated by the type of rule listed in a rule configuration file. A mapping between the XSD types describes rules and the java classes used to implement the rule processing mechanisms is required. For every concrete XSDType used to implement a processingMechanismConfigurationType, the event processor must have a mapping to an available java class. The XSDType: Java Class mappings are done by creating sets of matching pair entries in the <Attributes > element below: 1. The first is a <string> element with a name of "EPMechanismXSDType.N" where N is a positive integer. The value

Name	Description
	of the entry indicates the full URI of the type name, including the namespace. 2. The second is an <string> element named "EPMechanismClassName.N" where N matches the appropriate EPMechanismXSDType entry. The Event Processor will incrementally search for XSDType->Class mappings, beginning with an "N" of 1 and working incrementally positive until it can't find a type or class for the current N.</ string></string ></Attributes>
EP transport address	This field is not used for System Manager.

Button	Description
Edit	Opens the Edit Profile: Event processor page. Use this page to edit the parameters in the Event processor profile.
Done	Closes the View Profile: Event processor page.

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Alarm Management field descriptions on page 721
View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734
View Profile: User Bulk Import Profile field descriptions on page 759

View profile:Inventory field descriptions

To navigate to this page, click **Services** > **Configurations** > **Settings** > **Inventory** > **Configuration**.

General Properties

Name	Description
Maximum number of threads for the step Collecting Inventory Information	Specifies the maximum number of Java threads created and used for the step Collecting Inventory Information.

Name	Description
Maximum number of threads for the step Probing Network Elements	Specifies the maximum number of Java threads created and used for the step Probing Network Elements.
Maximum Records on single page of table	Specifies the total number of rows displayed in a table.

Button	Description
Edit	Takes you to the Edit Profile: Configuration page in **Inventory**.
Done	Closes the View Profile: Configuration page.

Edit Profile: Inventory field descriptions

General Properties

Name	Description
Maximum number of threads for the step Collecting Inventory Information	Specifies the maximum number of Java threads created and used for the step Collecting Inventory Information.
Maximum number of threads for the step Probing Network Elements	Specifies the maximum number of Java threads created and used for the step Probing Network Elements.
Maximum Records on single page of table	Specifies the total number of rows displayed in a table.

Button	Description
Commit	Saves the changes and closes the Edit Profile: Configuration page
Cancel	Cancels your action and takes you to the previous page.

View Profile : Data Transport Config field descriptions

Use this page to view the parameters and their values that are set for data transport configuration.

Name	Description
Connection Avaya production FQDN	The value is a fully qualified domain name of the target Enterprise for a connection. This may identify a customer, Business Partner or Avaya itself. For example, avaya.com, company.com
Connection Avaya production keyAlias	The value specifies the alias of a key in the keyStore to be used for client authentication in HTTPS sessions when communicating with an upstream server. Typically used when Avaya is the upstream server. This is an optional field.
Connection Avaya production platform qualifier	The value is a logical name for the target enterprise, that applies irrespective of primary of backup. The primary and backup are a part of the same organization. Components use this name to address the Enterprise Server pair. This name must match the name that the Enterprise Servers have assigned to themselves locally or else the connection is rejected.
Connection Avaya production primary URL	The value is a primary URL of the platform
Connection Avaya production useProxy	The value specifies whether to use proxies for this platform or not. The values are true or false.
Connection set	The set of connections that this SAL data transport will open. Each connection must have PlatformName, TargetFQDN, and PrimaryURL elements. Connections can optionally also have BackupURL elements.
Https session timeout	The value specifies the maximum duration of HTTPS authentication sessions before they need to be re-negotiated.
Max message exchange size	The value specifies maximum size of the messages data transport attempts to send or receive in one bundle. The following are the units of size: • B for bytes • M for megabytes • k for kilobytes

Name	Description
	Note: Do not change the default value unless there is a need.
Max queue memory	The value specifies the maximum amount of memory on disk that the queue can occupy. The following are the units of memory: • B for bytes • M for megabytes • k for kilobytes **Note:** Do not change the default value unless there is a need.
Max send transaction time	The value specifies the maximum amount of time spent in a transaction when trying to send upstream. **Note:** Do not change the default value unless there is a need.
Organization FQDN	The value specifies a fully qualified domain name that uniquely identifies the business organization that the SAL Platform resides in.
Polling interval	The time between polling for messages from each enterprise platform. Specify 0 to turn polling off. The following are the units: • h for Hours • m for Minutes The Agent polls because there is no way to connect directly from Avaya to the customer. Connections may only be initiated from the customer side. A component in the Enterprise can just send a message. The message is queued until either a message or a polling request is received from the destination Agent and the queued message is sent back to the Agent in the HTTPS reply.

Name	Description
Proxy address	The domain name or IP address of the proxy to use.
Proxy password	The password to use with the proxy. They are stored in a plain text.
Proxy port	The port of the proxy server.
Proxy type	The type of proxy based on whether the proxy supports HTTP or SOCKS.
Proxy use authentication	The value specifies whether an authentication is required to access the proxy server. The values are true and false. If the value is true, an authentication is required to access the server.
Proxy user	
Server status reset interval	The time between the server marking an URL as unreachable and reattempting to connect to that URL. The following are the units of time: • h for hours • m for minutes • s for seconds
SAL platform qualifier	A logical name for the target Enterprise, that applies irrespective of primary of backup. Implicitly, the primary and backup are a part of the same organization. Components use this name to address the Enterprise Server pair. This name must match the name that the Enterprise Servers have assigned to themselves locally or else the connection will be rejected.

Button	Description
Edit	Opens the Edit Profile: Data Transport Config page. Use this page to edit the parameters in the Data Transport Configuration profile.
Done	Closes the View Profile: Data Transport Config page.

Related topics:

View Profile: Agent Management field descriptions on page 720

View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734
View Profile: User Bulk Import Profile field descriptions on page 759

View Profile: Data Transport Static Config field descriptions

Do not change any values in the fields displayed on this page. Any change is likely to break the SAL Agent application.

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile : Data Transport Config field descriptions on page 728
View software feature profiles on page 734
View Profile: User Bulk Import Profile field descriptions on page 759

View Profile System Manager field descriptions

applicationMetadata

Name	Description
Version Detail	The build version of the System Manager.

database

Name	Description
connection_url	The complete URL for connecting to the database
hostname	Name of the computer that hosted the database
jdbc_class	Name of the database driver implementation class
password	Password for accessing the database
port	Port for the database connection
user	Name of the database user

Name	Description
vendor	Name of the database

Button	Description
Edit	Opens the Edit Profile System Manager page
Done	Closes the page.

Related topics:

View global feature profiles on page 719

Edit Profile System Manager field descriptions

applicationMetadata

Name	Description
Version Detail	The build version of the System Manager.

database

Name	Description
connection_url	Complete URL for connecting to the database
hostname	Name of the computer that hosted the database
jdbc_class	Name of the database driver implementation class
password	Password for accessing the database
port	Port for the database connection
user	Name of the database user
vendor	Name of the database

Button	Description
Commit	Saves changes to the database
Cancel	Takes you back to the View Profile: System Manager page

Related topics:

Edit global feature profiles on page 719

Edit software feature profiles

Service Profile Manager maintains the following software feature profiles for global feature profiles in System Manager:

To modify the software feature profiles, you must log in as administrator.

Edit Profile:Licenses field descriptions on page 739

Edit Profile:Alarming UI field descriptions on page 736

Edit Profile: SMGR Element Manager field descriptions on page 749

Edit Profile:Logging field descriptions on page 741

Edit Profile:Scheduler field descriptions on page 755

Edit Common Console Profile field descriptions on page 737

Edit Profile: Communication System Management Configuration field descriptions on page 725

Edit Profile User Bulk Import Profile field descriptions on page 762

Edit Profile: Role Bulk Import Profile field descriptions on page 746

View software feature profiles

Service Profile Manager maintains the following software feature profiles for global feature profiles in System Manager:

View Profile:Licenses field descriptions on page 738

View Profile:Alarming UI field descriptions on page 735

View Profile: SMGR Element Manager field descriptions on page 751

View Profile:Logging field descriptions on page 739

View Profile:Scheduler field descriptions on page 754

View Profile:SNMP field descriptions on page 753

View Common Console Profile field descriptions on page 736

View Profile: Communication System Management Configuration field descriptions on page 724

View Profile: Role Bulk Import Profile field descriptions on page 744

View Profile: User Bulk Import Profile field descriptions on page 759

View Profile:Alarming UI field descriptions

Use this page to view the parameters in the Alarming profile.

Color Codes

Name	Description
Cleared	The color code for cleared alarms.
Critical	The color code for critical alarms.
Intermediate	The color code for the intermediate alarms.
Major	The color code for the major alarms.
Minor	The color code for the minor alarms.
Warning	The color code for the warning alarms.

Auto Refresh

Name	Description
Time Interval (millisec)	The time interval in milliseconds after which the Alarming module refreshes the alarms on the Alarming page.

Button	Description
Edit	Opens the Edit Profile:Alarming UI page. Use this page to edit the parameters in the Alarming Profile.
Done	Closes the View Profile:Alarming UI page.

Related topics:

[View Profile: Agent Management field descriptions](#) on page 720
[View Profile: Alarm Management field descriptions](#) on page 721
[View Profile: Event processor field descriptions](#) on page 726
[View Profile : Data Transport Config field descriptions](#) on page 728
[View Profile: Data Transport Static Config field descriptions](#) on page 732
[View software feature profiles](#) on page 734
[View Profile: User Bulk Import Profile field descriptions](#) on page 759

Edit Profile:Alarming UI field descriptions

Use this page to edit the parameters in the Alarming profile.

Color Codes

Name	Description
Cleared	The color code for alarms that are cleared.
Critical	The color code for critical alarms.
Intermediate	The color code for the intermediate alarms.
Major	The color code for the major alarms.
Minor	The color code for the minor alarms.
Warning	The color code for the warning alarms.

Auto Refresh

Name	Description
Time Interval (millisec)	The time interval in milliseconds after which the Alarming module refreshes the alarms on the Alarming page.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Alarming UI page.

Related topics:

Edit software feature profiles on page 734
Edit Profile:Logging Service field descriptions on page 743

View Common Console Profile field descriptions

Use this page to view the common console profile.

Name	Description
Max No of tabs that can be opened on landing page	The maximum number of tabs that you can open from the home page. The default is 5.

Name	Description
Number of rows	Number of rows that you want the system to display in a table. The default count is 15 . The range of minimum rows is 15 and maximum rows is 100.
Max No of Records Selectable (Table)	The maximum number of records that you can select at a time from a table.

Button	Description
Edit	Opens the Edit Profile: Common Console page. Use this page to edit the parameters in the Common Console profile.
Done	Closes the View Profile: Common Console page.

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734
View Profile: User Bulk Import Profile field descriptions on page 759

Edit Common Console Profile field descriptions

Use this page to edit the common console profile.

Name	Description
Max No of tabs that can be opened on the landing page	The maximum number of tabs that you can open from the home page. The default is 5.
No Of Rows	The number of rows that you want the system to display in the table. The default count is 15. The range of minimum rows is 15 and maximum rows is 100.
Max No of Records Selectable (Table)	The maximum number of records that you can select at a time from a table.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation.

Related topics:

Edit software feature profiles on page 734
Edit Profile:Logging Service field descriptions on page 743

Configuring the UCM services

Procedure

1. On the System Manager console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR**.
3. Click **Common Console**.
4. On the View Profile: Common Console page, set the **UCM Configured** field to **true**.
5. Click **Done**.
   The system displays the links for the UCM services in the home page. Click on the relevant links to launch UCM.

View Profile:Licenses field descriptions

Use this page to view the parameters in the WebLM profile.

Name	Description
WebLM.Usages.UsageCount	This count represents the number of usage reports the server must maintain and display for each WebLM server.
WebLM.LicenseAllocation.Backup.FileSize	This property specifies the size of the license allocation backup file in MB. Allocate an integer to this property like 1 or 10. A decimal value like 1.5 is not valid.

Button	Description
Edit	Opens the Edit Profile:Licenses (WebLM) page. Use this page to edit the parameters in the WebLM profile.
Done	Closes the View Profile:Licenses (WebLM) page.

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734
View Profile: User Bulk Import Profile field descriptions on page 759

Edit Profile:Licenses field descriptions

Use this page to edit the parameters in the WebLM profile.

Name	Description
WebLM.Usages.UsageCount	This count represents the number of usage reports the server must maintain and display for each WebLM server.
WebLM.LicenseAllocation.Backup.FileSize	This property specifies the size of the license allocation backup file in MB. Allocate an integer to this property like 1 or 10. A decimal value like 1.5 is not valid.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Licenses (WebLM) page.

Related topics:

Edit software feature profiles on page 734
Edit Profile:Logging Service field descriptions on page 743

View Profile:Logging field descriptions

Use this page to view the parameters in the Logging profile.

Log Severity Levels

Name	Description
Alert	The color code for the log messages that are logged under the Alert severity level.
Critical	The color code for the log messages that are logged under the Critical severity level.
Debug	The color code for the log messages that are logged under the Debug severity level.
Emergency	The color code for the log messages that are logged under the Emergency severity level.
Error	The color code for the log messages that are logged under the Error severity level.
Informational	The color code for the log messages that are logged under the Informational severity level.
Notice	The color code for the log messages that are logged under the Notice severity level.
Warning	The color code for the log messages that are logged under the Notice severity level.

Auto Refresh

Name	Description
auto_refresh_time_interval	The time interval in milliseconds after which the log messages are auto refreshed on the Logging page .

Button	Description
Edit	Opens the Edit Profile:Logging page. Use this page to edit the parameters in the Logging profile.
Done	Closes the View Profile:Logging page.

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734

View Profile: User Bulk Import Profile field descriptions on page 759

Edit Profile:Logging field descriptions

Use this page to edit the parameters in the Logging profile.

Log Severity Levels

Name	Description
Alert	The color code for the log messages that are logged under the Alert severity level.
Critical	The color code for the log messages that are logged under the Critical severity level.
Debug	The color code for the log messages that are logged under the Debug security level.
Emergency	The color code for the log messages that are logged under the Emergency severity level.
Error	The color code for the log messages that are logged under the Error severity level.
Informational	The color code for the log messages that are logged under the Informational severity level.
Notice	The color code for the log messages that are logged under the Notice severity level.
Warning	The color code for the log messages that are logged under the Notice severity level.

Auto Refresh

Name	Description
auto_refresh_time_interval	The time interval in milliseconds after which the log messages are auto refreshed on the Logging page .

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Logging page.

View Profile:Logging Service field descriptions

Use this page to view the parameters and their corresponding values that specify the default settings for log harvesting service.

Name	Description
Max time interval to wait	The maximum time interval for which the system waits between a request and a response for harvesting a log file from a remote System Manager computer. You can specify a time interval between 1800000 milliseconds to maximum value of 7200000 milliseconds. The default value is 10800000 milliseconds.
Size of the File Buffer	The value in this field is the buffer size for the files displayed to the log harvesting user interface. The minimum size of the file buffer is 10000 bytes and maximum value is 5000000 bytes.
Size of the LRU buffer cache	The value in this field is the size of the cache. The files that you view or search are temporarily stored in the cache. If you open a file after the cache becomes full, the least recently used file is removed from the cache and the new file is stored in the cache. The system takes less time to open and display a file that is in cache.
Directory path for harvested files	The directory where all the harvested files are stored. The default path is `/var/log/Avaya/mgmt/downloads`.
Number of Lines in a Log Browser page (Requires Service Restart)	The value is the maximum number of lines that you can view on the log browser page for a harvested log file.
Maximum allowed size of harvest directory	The maximum size of the harvested files directory. The value of minimum size of the harvested directory is 1 GB and maximum size can be 10 GB.
No. of files for File rotation	The maximum number of harvested files that the system can store before the oldest file is overwritten by the new harvested file. You can set 10 as minimum number of files and 9999999 as maximum number of files.

Button	Description
Edit	Opens the Edit Logging Service Profile page. Use this page to edit the values of the log harvesting parameters.
Done	Closes the View Logging Service Profile page.

Edit Profile:Logging Service field descriptions

Use this page to modify the value of parameters that define settings for log harvesting.

Name	Description
Max time interval to wait	The maximum time interval for which the system waits between a request and a response for harvesting a log file from a remote System Manager computer. You can specify a time interval between 1800000 milliseconds to maximum value of 7200000 milliseconds. The default value is 10800000 milliseconds.
Size of the File Buffer	The value in this field is the buffer size for the files displayed to the log harvesting user interface. The minimum size of the file buffer is 10000 bytes and maximum value is 5000000 bytes.
Size of the LRU buffer cache	The value in this field is the size of the cache. The files that you view or search are temporarily stored in the cache. If you open a file after the cache becomes full, the least recently used file is removed from the cache and the new file is stored in the cache. The system takes less time to open and display a file that is in the cache.
Directory path for harvested files	The directory where all the harvested files are stored. The default path is `/var/log/Avaya/mgmt/downloads`.
Number of Lines in a Log Browser page (Requires Service Restart)	The value is the maximum number of lines that you can view on the log browser page for a harvested log file.
Maximum allowed size of harvest directory	The maximum size of the harvested files directory. The value of minimum size of the harvested directory is 1 GB and maximum size can be 10 GB.

Name	Description
No. of files for File rotation	The maximum number of harvested files that the system can store before the oldest file is overwritten by the new harvested file. You can set 10 as minimum number of files and 9999999 as maximum number of files.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Logging Service page.

Related topics:

Edit software feature profiles on page 734

View Profile: Role Bulk Import Profile field descriptions

Use this page to view the parameters and their corresponding values that specify bulk import settings for importing roles records.

Role Bulk Import Module

Name	Description
Default Error Configuration	The value in this field specifies what action the system performs when an error is encountered during bulk importing roles record in the system. The options are: • True: When this parameter is set to true, the system skips the erroneous record in the input file and continue to import other records. This is the default value. If this parameter is set to true, the **Continue processing other records** option is set as the default option for the **Select error configuration** field on the Import Roles page. • False: When this parameter is set to false, the system aborts the importing process on encountering the first error in the input file. If this parameter is set to false, the **Abort on first error** option is set as default option

Name	Description
	for the **Select error configuration** field on the Import Roles page. To access the Import Roles page, click **Groups & Roles** > **More Actions** > **Import Roles**.
Schedule Job	The value in this field specifies the default scheduling option for importing a roles job. The options are: • True: When this parameter is set to true, the system run the bulk importing roles job immediately. This is the default value. If this parameter is set to true, the **Run immediately** option is set as the default option for the **Schedule job** field on the Import Roles page. • False: When this parameter is set to false, you can set the date and time of running the bulk importing roles job. If this parameter is set to false, the **Schedule later** option is set as the default option for the **Schedule job** field on the Import Roles page. To access the Import Roles page, click **Groups & Roles** > **More Actions** > **Import Roles**.
Maximum Number of Error records to be displayed	The value in this field specifies the maximum number of error records that the Job Details page can display for a role importing job that has failed. To access the Job Details page, click **Groups & Roles** > **More Actions** > **Import Roles** > **View Job**. Select a failed job from the table before you click **View Job**.
Maximum Number of Job records to be displayed	The value in this field specifies the maximum number of job records that the system displays on the Import Roles page.
Default Action for a matching record	The value specifies a default action that the system performs when the system finds a matching record in the database while bulk importing roles. The options are: • 0: When you set 0 for this parameter, the system does not import role records from

Name	Description
	the input file that already exists in the database. If you enter 0, the **Skip** option is set as the default option for the **If a matching record already exists** field on the Import Roles page.. • 1: When you set 1 for this parameter, the system appends the records for an attribute. If you enter 1, the **Merge** option is set as the default option for the **If a matching record already exists** field on the Import Roles page.. • 2: When you set the value of this parameter to 2, the system replaces the record with the record in the input file if a matching record is found. If you enter 2, the **Replace** option is set as the default option for the **If a matching record already exists** field on the Import Roles page. • 3: When you set the value of this parameter to 3, the system deletes the records from the database that matches the records in the input file. If you enter 3, the **Delete** option is set as the default option for the **If a matching record already exists** field. To access the Import Roles page, click **Groups & Roles** > **More Actions** > **Import Roles**.

Button	Description
Edit	Opens the Edit Profile:Role Bulk Import Profile page. You can use this page to modify the values set for the role bulk import parameters.

Edit Profile: Role Bulk Import Profile field descriptions

Use this page to modify the value of parameters that define settings for bulk importing role records.

Role Bulk Import Module

Name	Description
Default Error Configuration	The value in this field specifies what action the system performs when an error is encountered during bulk importing roles record in the system. The options are: • True: When this parameter is set to true, the system skips the erroneous record in the input file and continue to import other records. This is the default value. If this parameter is set to true, the **Continue processing other records** option is set as the default option for the **Select error configuration** field on the Import Roles page. • False: When this parameter is set to false, the system aborts the importing process on encountering the first error in the input file. If this parameter is set to false, the **Abort on first error** option is set as default option for the **Select error configuration** field on the Import Roles page. To access the Import Roles page, click **Groups & Roles** > **More Actions** > **Import Roles**.
Schedule Job	The value in this field specifies the default scheduling option for importing a roles job. The options are: • True: When this parameter is set to true, the system run the bulk importing roles job immediately. This is the default value. If this parameter is set to true, the **Run immediately** option is set as the default option for the **Schedule job** field on the Import Roles page. • False: When this parameter is set to false, you can set the date and time of running the bulk importing roles job. If this parameter is set to false, the **Schedule later** option is set as the default option for the **Schedule job** field on the Import Roles page.

Name	Description
	To access the Import Roles page, click **Groups & Roles** > **More Actions** > **Import Roles**.
Maximum Number of Error records to be displayed	The value in this field specifies the maximum number of error records that the Job Details page can display for a role importing job that has failed. To access the Job Details page, click **Groups & Roles** > **More Actions** > **Import Roles** > **View Job**. Select a failed job from the table before you click **View Job**.
Maximum Number of Job records to be displayed	The value in this field specifies the maximum number of job records that the system displays on the Import Roles page.
Default Action for a matching record	The value specifies a default action that the system performs when the system finds a matching record in the database while bulk importing roles. The options are: • 0: When you set 0 for this parameter, the system does not import role records from the input file that already exists in the database. If you enter 0, the **Skip** option is set as the default option for the **If a matching record already exists** field on the Import Roles page.. • 1: When you set 1 for this parameter, the system appends the records for an attribute. If you enter 1, the **Merge** option is set as the default option for the **If a matching record already exists** field on the Import Roles page.. • 2: When you set the value of this parameter to 2, the system replaces the record with the record in the input file if a matching record is found. If you enter 2, the **Replace** option is set as the default option for the **If a matching record already exists** field on the Import Roles page. • 3: When you set the value of this parameter to 3, the system deletes the records from

Name	Description
	the database that matches the records in the input file. If you enter 3, the **Delete** option is set as the default option for the **If a matching record already exists** field. To access the Import Roles page, click **Groups & Roles** > **More Actions** > **Import Roles**.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the Edit Profile: Role Bulk Import Profile page.

Edit Profile: SMGR Element Manager field descriptions

Use this page to edit the parameters in the SMGR Element Manager profile.

Name	Description
Backup Directory	The name of the directory on the Database server where Element Manager creates the backup archives. **Note:** The database user must have write privileges on this directory.
Database Utilities Path	The name of the directory on the Database server that contains the PostgreSQL backup/restore utilities. **Note:** The database user must have execute permissions on these utilities.
Database Type	Type of the database. For example, Oracle, Postgres.
Database server	Host name of the database server.
Database Super-User Password	Database super user password.
Database Port	Port number for database server.

Name	Description
Database SCP Port	Port on the database server on which the SSH server is running.
Database Super-User	Database super user. This user should be able to open a SSH connection to the DB.
Disk Space Allocated (GB)	Disk space allocated for backup archives.
Disk Space Threshold (%)	This is the percentage of the **diskSpaceAllocated** property. When this percentage is reached, an alarm is generated. So, if the **diskSpaceAllocated** is 100 MB and **diskSpaceThreshold** is 90 percent, an alarm is generated when the disk space occupied by the backup archives reaches 90 MB.
Job Interface URL	Lookup URL for the Element Manager.
Maximum Backup Files	The maximum number of backup files that you can create. Once maximum limit is reached, the backup archives are rotated.
Maximum Data Retention Limit (days)	The maximum data retention limit that can be set for any data retention rule in days.
Maximum size for log data stored	The maximum size for log data stored. This is the upper limit on the number of records on the log_store table.
Maximum Transaction Timeout Limit (Hours)	The maximum transaction timeout limit in hours.
Remote Utility Directory	Directory on the database server that contains the Element Manager backup/ restore utilities.
Scheduler URL	The URL for accessing the Scheduler.
Remote Server Password	Password for accessing the scp server. **Important:** To use the **Use Default** option on the Backup or Restore page, ensure that you specify the remote server IP, user name, password, and name and path of the backup file on this page.
Remote Server Port	SSH port for the scp server.
Remote server	Host name of the scp server.
Remote Server User	User name for accessing the secure access server.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation for IMSM Element Manager and takes you back to the View Profile: IMSM Element Manager page.

Related topics:

Edit software feature profiles on page 734
Edit Profile:Logging Service field descriptions on page 743

View Profile: SMGR Element Manager field descriptions

Use this page to view the parameters in the SMGR Element Manager profile.

Name	Description
Backup Directory	The name of the directory on the Database server where Element Manager creates the backup archives. **Note:** The database user must have write privileges on this directory.
Database Utilities Path	The name of the directory on the Database server that contains the PostgreSQL backup/restore utilities. **Note:** The database user must have execute permissions on these utilities.
Database Type	Type of the database. For example, Oracle, Postgres.
Database server	Host name of the database server.
Database Super-User Password	Database super user password.
Database Port	Port number for database server.
Database SCP Port	Port on the database server on which the SSH server is running.
Database Super-User	Database super user. This user must be able to open a SSH connection to the database.
Disk Space Allocated (GB)	Disk space allocated for backup archives.

Name	Description
Disk Space Threshold (%)	Percentage of the **diskSpaceAllocated** property. When this percentage is reached, the system generates an alarm. For example, if the **diskSpaceAllocated** is 100 MB and **diskSpaceThreshold** is 90 percent, the system generates an alarm when the disk space occupied by the backup archives reaches 90 MB.
Job Interface URL	Lookup URL for the Element Manager.
Maximum Backup Files	The maximum number of backup files that you can create. When the maximum limit is reached, the backup archives are rotated.
Maximum Data Retention Limit (days)	The maximum data retention limit in days that you can set for any data retention rule.
Maximum size for log data stored	The maximum size for log data stored. This is the upper limit on the number of records on the log_store table.
Maximum Transaction Timeout Limit (Hours)	The maximum transaction timeout limit in hours
Remote Utility Directory	Directory on the database server that contains the Element Manager backup or restore utilities.
Scheduler URL	The URL for gaining access to the Scheduler.
Remote Server Password	Password for accessing the scp server. **Important:** To use the **Use Default** option on the Backup or Restore page, ensure that you specify the remote server IP, user name, password, and name and path of the backup file on this page.
Remote Server Port	SSH port for the scp server.
Remote server	Host name of the scp server.
Remote Server User	User name for accessing the secure access server.

Button	Description
Edit	Opens the Edit Profile:IMSM Element Manager page. Use this page to edit the

Button	Description
	parameters in the IMSM Element Manager Profile.
Done	Closes the View Profile:IMSM Element Manager page.

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734
View Profile: User Bulk Import Profile field descriptions on page 759

View Profile:SNMP field descriptions

Use this page to view the parameters in the SNMP profile.

Avaya IM System Manager subagent attributes

Name	Description
Master Agent IPAddress	IP address of machine on which master agent is running.
Master Agent TCP Port	The connection between master agent and subagent is established via a TCP port using AgentX protocol. This port has to be configured with both the master agent and the subagent so that the master agent starts listening on the configured TCP port and then the subagent establishes connection with the master agent via this port.
Sub Agent IPAddress	IP address of machine on which sub agent is deployed

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734

View Profile: User Bulk Import Profile field descriptions on page 759

Edit Profile:SNMP field descriptions

Use this page to edit the parameters in the SNMP profile.

Avaya IM System Manager subagent attributes

Name	Description
Master Agent IPAddress	IP address of machine on which master agent is running.
Master Agent TCP Port	The connection between master agent and subagent is established via a TCP port using AgentX protocol. This port has to be configured with both the master agent and the subagent so that the master agent starts listening on the configured TCP port and then the subagent establishes connection with the master agent via this port.
Sub Agent IPAddress	IP address of machine on which sub agent is deployed

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile: SNMP page.

Related topics:

Edit software feature profiles on page 734
Edit Profile:Logging Service field descriptions on page 743

View Profile:Scheduler field descriptions

Use this page to view the parameters in the Scheduler profile.

Scheduler Feature

Name	Description
Number Of Retry	A count that defines the number of attempts to start the scheduler MBEAN.

Name	Description
Retry Delay	Delay in time in seconds between each retry.

Scheduler Look Up Details

Name	Description
Initial Context Factory	User name for secured Java Naming and Directory Interface (JNDI).
Naming Server User Name	
Provider URL	The PROVIDER_URL which gives the server name and port on which a service is running. **Note:** This parameter is currently not in use.

Button	Description
Edit	Opens the Edit Profile:Scheduler page. Use this page to edit the parameters in the Scheduler profile.
Done	Closes the View Profile:Scheduler page.

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734
View Profile: User Bulk Import Profile field descriptions on page 759

Edit Profile:Scheduler field descriptions

Use this page to edit the parameters in the Scheduler profile.

Scheduler Feature

Name	Description
Number Of Retry	A count that defines the number of attempts to start the scheduler MBEAN.

Name	Description
Retry Delay	Delay in time in seconds between each retry.

Scheduler Look Up Details

Name	Description
Initial Context Factory	User name for secured Java Naming and Directory Interface (JNDI).
Naming Server User Name	
Provider URL	The PROVIDER_URL which gives the server name and port on which a service is running. **Note:** This parameter is currently not in use.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Scheduler page.

Related topics:

Edit software feature profiles on page 734
Edit Profile:Logging Service field descriptions on page 743

Configuring the TrapListener service

Procedure

1. On the System Manager console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR**.
3. Click **TrapListener**.
4. On the View Profile: TrapListener Service page, click **Edit**.
5. Edit the required fields in the Edit Profile: TrapListener Service page.
6. Click **Commit**.

Related topics:

TrapListener service field descriptions on page 757

TrapListener service field descriptions

Name	Description
Authentication Password	The password used to authenticate the user.
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are: • **MD5 (default)** • **SHA** The default value is **MD5**.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Privacy Protocol	The encryption policy for an SNMP V3 user. The possible values are: • **DES**: Use DES encryption for SNMP based communication. • **AES**: Use AES encryption for SNMP based communication The default value is AES.
Port	The port on which TrapListener listens. Default value is 10162. This field is read-only.
V3 username	Specifies the SNMP V3 user name. Default value is initial.
Community	Specifies the community for the TrapListener.

Button	Description
Commit	Saves the changes you have made in the TrapListener Configuration Parameters section.
Cancel	Cancels the edit and takes you to the previous page.

Note:

For the **Privacy Password**, **Authentication Password**, **Users** and **Community** fields, the default value is configured. You should change these values immediately after you deploy System Manager.

Renewing identity certificates

Procedure

1. On the System Manager Web Console, click **Services** > **Configurations**.
2. Click **Settings** > **SMGR** > **Trust Management**.
3. On the View Profile: TrustManagement page click **Edit**.
4. Modify the auto renewal properties in the Edit Profile: TrustManagement page.
5. Click **Commit**.

   The certificates are renewed automatically according to the **Auto Renewal Threshold** you set.

Related topics:

View Profile: TrustManagement field descriptions on page 758
Edit Profile: TrustManagement field descriptions on page 759

View Profile: TrustManagement field descriptions

Name	Description
Auto Renewal Alarm Threshold	Number of days prior to the certificate expiry when an alarm is generated.
Auto Renewal Status	Status of the auto renewal of certificates from the Trust Management agent. Set this field to True if you want auto renewal of certificates.
Auto Renewal Threshold	Number of days prior to the certificate expiry when the auto renewal of certificates is triggered.

Button	Description
Edit	Takes you to the Edit Profile: TrustManagement page.

Button	Description
Done	Takes you back to the previous page.

Edit Profile: TrustManagement field descriptions

Name	Description
Auto Renewal Alarm Threshold	Number of days prior to the certificate expiry when an alarm is generated.
Auto Renewal Status	Status of the auto renewal of certificates from the Trust Management agent. Set this field to **True** if you want auto renewal of certificates.
Auto Renewal Threshold	Number of days prior to the certificate expiry when the auto renewal of certificates is triggered.

Button	Description
Commit	Saves your changes in the Edit Profile: TrustManagement page.
Cancel	Cancels your changes and takes you to the previous page.

View Profile: User Bulk Import Profile field descriptions

Use this page to view the parameters and their corresponding values that specify the default settings for bulk importing user records.

User Bulk Import Module

Name	Description
Default Error Configuration	The value in this field specifies what action the system performs when an error is encountered during bulk importing users record in the system. The options are: • True: When this parameter is set to true, the system skips the erroneous record in the input file and continue to import other records. This is the default value. If this parameter is set to true, the **Continue processing other records**

Name	Description
	option is set as the default option for the **Select error configuration** field on the Import Users page. • False: When this parameter is set to false, the system aborts the importing process on encountering the first error in the input file. If this parameter is set to false, the **Abort on first error** option is set as default option for the **Select error configuration** field on the Import Users page. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users**
Enable Error File Generation	The value in this field specifies the error file generation options for an importing users job. The options are: • True: When this parameter is set to true, the system generates an error file for a failed import. • False: When this parameter is set to false, the system does not generate an error file for a failed import.
Maximum Number of Error records to be displayed	The value in this field specifies the maximum number of error records that the Job Details page can display for a user importing job that has failed to import user records completely or partially. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users** > **View Job** Select a failed job from the table before you click **View Job**
Maximum Number of Job records to be displayed	The value in this field specifies the maximum number of job records that the system displays on the Import Users page.
Default Action for a matching record	The value specifies a default action that the system performs when the system finds a matching record in the database while bulk importing users. The options are: • 0: When you set 0 for this parameter, the system does not import user records from the input file that already exists in the database.

Name	Description
	If you enter 0, the **Skip** option is set as the default option for the **If a matching record already exists** field on the Import Users page.. • 1: When you set 1 for this parameter, the system appends the records for an attribute. If you enter 1, the **Merge** option is set as the default option for the **If a matching record already exists** field on the Import Users page.. • 2: When you set the value of this parameter to 2, the system replaces the record with the record in the input file if a matching record is found. If you enter 2, the **Replace** option is set as the default option for the **If a matching record already exists** field on the Import Users page. • 3: When you set the value of this parameter to 3, the system deletes the records from the database that matches the records in the input file. If you enter 3, the **Delete** option is set as the default option for the **If a matching record already exists** field. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users**

Button	Description
Edit	Opens the Edit Profile:User Bulk Import Profile page. You can use this page to modify the values set for the user bulk import parameters.

Related topics:

View Profile: Agent Management field descriptions on page 720
View Profile: Alarm Management field descriptions on page 721
View Profile: Event processor field descriptions on page 726
View Profile : Data Transport Config field descriptions on page 728
View Profile: Data Transport Static Config field descriptions on page 732
View software feature profiles on page 734

Edit Profile: User Bulk Import Profile field descriptions

Use this page to modify the value of parameters that define settings for bulk importing users records.

User Bulk Import Module

Name	Description
Default Error Configuration	The value in this field specifies what action the system performs when an error is encountered during bulk importing users record in the system. The options are: • True: When this parameter is set to true, the system skips the erroneous record in the input file and continue to import other records. This is the default value. If this parameter is set to true, the **Continue processing other records** option is set as the default option for the **Select error configuration** field on the Import Users page. • False: When this parameter is set to false, the system aborts the importing process on encountering the first error in the input file. If this parameter is set to false, the **Abort on first error** option is set as default option for the **Select error configuration** field on the Import Users page. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users**
Enable Error File Generation	The value in this field specifies the error file generation options for an importing users job. The options are: • True: When this parameter is set to true, the system generates an error file for a failed import. • False: When this parameter is set to false, the system does not generate an error file for a failed import.
Maximum Number of Error records to be displayed	The value in this field specifies the maximum number of error records that the Job Details page can display for a user importing job that

Name	Description
	has failed to import user records completely or partially. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users** > **View Job** Select a failed job from the table before you click **View Job**
Maximum Number of Job records to be displayed	The value in this field specifies the maximum number of job records that the system displays on the Import Users page.
Default Action for a matching record	The value specifies a default action that the system performs when the system finds a matching record in the database while bulk importing users. The options are: • 0: When you set 0 for this parameter, the system does not import user records from the input file that already exists in the database. If you enter 0, the **Skip** option is set as the default option for the **If a matching record already exists** field on the Import Users page.. • 1: When you set 1 for this parameter, the system appends the records for an attribute. If you enter 1, the **Merge** option is set as the default option for the **If a matching record already exists** field on the Import Users page.. • 2: When you set the value of this parameter to 2, the system replaces the record with the record in the input file if a matching record is found. If you enter 2, the **Replace** option is set as the default option for the **If a matching record already exists** field on the Import Users page. • 3: When you set the value of this parameter to 3, the system deletes the records from the database that matches the records in the input file. If you enter 3, the **Delete** option is set as the default option for the **If a matching record already exists** field.

Name	Description
	To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users**

Button	Description
Edit	Opens the Edit Profile:User Bulk Import Profile page. You can use this page to modify the values set for the user bulk import parameters.

Chapter 9: Managing events

Managing alarms

Alarming

The Alarming service provides an interface for monitoring alarms generated by System Manager and other components. You can:

- View an alarm.
- Change the status of an alarm.
- Export alarms to a Comma Separated Values (.csv) file through the Alarming service.

System Manager generates alarms to notify users of system events. Alarms are classified by their effect on system operation. Alarms can also identify the system component that generated the alarm.

Note:

- For Release 6.1 elements with 6.1 SAL agent, and Release 6.2 elements with 6.2 serviceability agent, System Manager cannot forward traps to NMS. You can configure 6.1 elements with 6.1 SAL agent and 6.2 elements with 6.2 serviceability agent to send SNMP traps directly to a customer Network Management System (NMS).

  However, for Release 6.2 elements, you can configure from System Manager instead of configuring in each element.
- For Release 5.2 elements and Release 6.0 elements, you can configure System Manager to forward alarms to Avaya Data Center (ADC).

For information on configuring, see the section “Managing Serviceability Agents” in chapter “Managing Elements”.

Viewing alarms

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select an alarm from the Alarm List. You can select multiple alarms.
4. Click **View**.
   The system displays the alarm details on the Alarm - View Alarm Detail page.

Changing the alarm status

The status of an alarm can be:

- **Acknowledged**: Maintenance support must manually set the alarm to this state. Indicates the alarm is under investigation.
- **Cleared**: Maintenance support must manually set the alarm to this state. Indicates the error condition has been resolved.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select an alarm and click **Change Status**.
   You can select multiple alarms.
4. Click the status that you want to apply to the selected alarms.

Exporting alarms

You can export alarms to a Comma Separated Values (.csv) file. You can open the CSV file using a text editor such as Wordpad or a spreadsheet application such as Microsoft Excel.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.

2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, perform one of the following steps:
   - To export an alarm to a CSV file, select an alarm and click **More Actions** > **Export Selected**.
   - To export all the alarms to a CSV file, click **More Actions** > **Export All**.
4. Click **Save** to save the exported file to the local disk.

Filtering alarms

The criteria for filtering the alarms are Severity, Status, Host Name, Message, Identifier, and M/E Ref Number. You can use more than one filter criterion on the selected alarms.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select the alarms you want to filter.
4. Click **Filter: Enable** at the top right corner of the Alarm List table.
5. Select the filter criteria you want to apply to the selected alarms.

   The **Status** and **Severity** fields have drop-down menus.

   You can enter the alarm code in the Message field to find all alarms which contain a particular alarm code.
6. Click **Filter: Apply**.

   Note:

   The system displays a message if no records are found which match the specified filter criteria.

Result

The system displays the alarms that match the filter criteria.

Searching for alarms

Use the Advanced Search function to find alarms based on certain specified conditions. The system displays only those alarms which satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, click **Advanced Search**.
4. In the **Criteria** section, from the first and second drop-down fields, select the search criterion and the operator.

   The default value in the first drop-down field is **Time Stamp**.
5. Select or enter the search value in the third field.
6. To add another search condition, click **+** and perform the following:

   a. Select the AND or OR operator from the drop-down field.
   b. Repeat Step 4 and Step 5.

   To delete a search condition, click **-**. You can delete a search condition only if you added more than one search condition.
7. To find alarms for the given search conditions, click **Search**.

Alarming field descriptions

The Alarming page displays a list of alarms. Use this page to view the alarms in the **Auto-Refresh** mode. In this mode, the page updates the alarm information automatically.

Field	Description
Time Stamp	Specifies the date and time when the alarm is generated.
Severity	Specifies the severity of the alarm.
Status	Specifies the current status of the alarms.
Host Name/SysName	Specifies the name of the host computer that generated the alarm.
Description	A detailed description of the problem that generated the alarm.
M/E Ref Number/SysOID	Specifies the unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. For alarms that are generated from trap listener, the system displays the System OID.

Field	Description
Identifier	Specifies the unique identifier for an alarm.
NotificationOID	Specifies the SNMP OID of the alarm.

Button	Description
Alarm landing Page	Changes the mode from **Auto-Refresh** to Manual refresh and displays the Alarming home page. This is a toggle button.

Alarming field descriptions

The Alarming home page has two sections: upper and lower. The upper section has buttons that you can use to view the details of the selected alarms, change the status of alarms, search for alarms , and set filters to view specific alarms. The lower section displays alarms in a table. The table provides information about the status of the alarms along with their severity. You can click a column title to sort the information in the table in ascending or descending order.

Field	Description
Time Stamp	Specifies the date and time when the alarm is generated.
Severity	Specifies the severity of the alarm.
Status	Specifies the current status of the alarms.
Host Name / SysName	Specifies the name of the host server that generated the alarm. In case of the trap listener service, this column specifies the system name.
Source IP Address	Specifies the IP address of the system that generated the alarm.
Description	Provides a detailed description of the problem that generated the alarm.
M/E Ref Number / SysOID	Specifies the unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. For alarms that are generated from trap listener, the system displays the System OID.
Identifier	Specifies the unique identifier for an alarm.
Event ID	Specifies the log event ID if the alarm is generated from logs or the Event OID if the

Field	Description
	alarm is generated from the trap listener service.
NotificationOID	Specifies the SNMP OID of the alarm.

Button	Description
View	Displays the details of the selected alarms.
Change Status	Changes the status of the selected alarm. The options are: • **Acknowledged** • **Cleared**
Auto-Refresh Mode	Changes over to the **Auto-Refresh** mode. When the Alarming page is set in this mode, it automatically updates the alarms in the table. A toggle button.
More Actions > **Export Selected**	Exports the selected alarms to a CSV file, which can be viewed with Wordpad or Excel.
More Actions > **Export All**	Exports all the alarms to a CSV file, which can be viewed with Wordpad or Excel.
Advanced Search	Displays fields that you can use to specify the search criteria for searching an alarm.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. A toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. A toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters alarms based on the filter criteria.
All	Selects all the alarms in the table.
None	Clears the check box selections.
Previous	Displays the logs in the previous page. This button is not available if you are on the first page.
Next	Displays the logs in the next page. This button is not available if you are on the last page.

Criteria section

This section appears when you click **Advanced Search** on the upper right corner of page.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Criteria</td><td>Use this section to specify search conditions. Select the search criteria from the first drop-down list. Select the operator from the second drop-down list. Enter the search value in the text field.
Select following search criteria from the first drop-down list:
Time Stamp: Searches all of the alarms that match the specified date and time. The valid format for entering the date is MM/DD/YYYY. The valid format for entering the time is HH:MM.
Severity: Searches all the alarms that match the specified severity level.
Status: Searches all the alarms that match the specified status.
Host Name: Searches all of the alarms that are generated from the specified host.
Identifier: Searches all the alarms that match the specified identifier.
Description: Searches all the alarms that match the specified description.
M/E Ref Number: Searches all the alarms that match the specified M/E Ref Number.
The operators available are based on the search criterion that you select in the first drop-down field. The following table lists the operators that are available for a search criterion:<table><tr><th>Criterion</th><th>Operators</th></tr><tr><td>Time Stamp</td><td>=, >, <, >=, <=, >=, !=</td></tr><tr><td>Severity</td><td>Equals, Not Equals</td></tr><tr><td>Status</td><td>Equals, Not Equals</td></tr></table></td></tr>
</table>

Name	Description
	<table><tr><th>Criterion</th><th>Operators</th></tr><tr><td>Host Name</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr><tr><td>Identifier</td><td>=, >, <, >=, <=, >=, !=</td></tr><tr><td>Description</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr><tr><td>M/E Ref Number</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr></table> When you select **Begin Date** and **End Date** from the first drop-down list, you are prompted to enter the date in the third field.

Button	Description
Clear	Clears the entered search criteria and sets the default search criteria.
Search	Searches the alarms based on the search conditions.
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	Deletes a search condition.

Managing logs

Logging Service

The Logging Service provides configuration capabilities and overall management of logs. The Logging Service receives and stores log events and harvests file-based logs or local database logs. You can view and monitor logs and their details through the log viewer. The log viewer is

integrated with the common console to provide consistent presentation of log messages for System Manager and the adopters.

The log viewer displays a list of logs where you can view the details of each log, perform a search for logs, and filter specific logs. Log details include information about the event that generates the log, the severity level of the log, and other relevant information. You can search logs based on search conditions and set filters to view logs that match the filter criteria.

The following are some of the log types that you may come across when viewing logs on the System Manager console:

- Security: Security loggers gather security logs.
- Audit: Audit loggers gather audit logs.
- Operation: Operational loggers gather operational logs.
- Debug: Debug loggers collect debug information to troubleshoot issues at the customer site.

The Logs menu in System Manager comprises of:

- Log Harvester: Through the Log Harvester menu you can harvest log files for one or more products of same or different types, running on the same computer or on different computers.
- Log Settings: This menu displays the loggers and appenders for the selected log configuration file. You can modify the logger and appender settings through this menu.
- Log Viewer: The log viewer allows you to view the logs generated by System Manager and other components and their details. You can view details of each log, perform a search for logs, and filter specific logs.

Log Types

Following are some of the log types that you may come across when viewing logs on the System Manager console. You can view the station-specific logs in the `/var/log/Avaya/mgmt/iptcm` directory.

Security

Security loggers gather security logs.

Audit

Audit loggers gather audit logs.

Operation

Operational loggers gather operational logs.

Debug

Debug loggers collect debug information to troubleshoot issues at the customer site. These loggers are categorized based on the Communication System Management components.

Debug.Station

Debug Station loggers gather debug information for station management related operations.

Debug.Template

Template Debug loggers gather debug information for template management related operations.

Debug.CM

CM debug loggers gather debug information for communication between Communication Manager and the Communication System Management server.

Debug.NCM

NCM debug logger gathers debug information related to Element Cut Through.

Debug.Synch

Synch debug logger gathers debug information for synchronization operations.

Debug.Model

Model debug logger gathers debug information for database operations.

Debug

Debug logger gathers debug information other than those gathered for the debug types mentioned above.

Managing log harvester

Log Harvester

Log harvesting is a service that manages the retrieval, archival, and analysis of harvested log files stored in Secure Access Link (SAL) agent enabled hosts or elements. The SAL agent harvests the logs and sends the harvested logs to the Logging Service through HTTPS. The logging service recognizes a successful harvest request related to a harvest profile, accepts the file segments, creates a well-defined file structure, and saves the request in the System Manager Node.

You can harvest log files for one or more products of the same or different types running on the same computer or on different computers. The system displays the list of file archives and respective profiles on the log harvesting user interface and the status of each archive is available in the user interface table.

You can perform the following operations through the log harvesting service:

- Create a log harvesting profile to specify the products for which you want to harvest the logs.
- Submit the log harvesting request defined in a profile to the product.

- View the status of the log harvesting request.
- Store the harvested log files of a product in an archive file.
- View the harvested log files stored in the archive file.
- Download the harvested log files on to a local computer.
- Search for a matching text in the harvested log files.

Accessing the Log Harvester service

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.

Result

The system displays the **Log Harvester** page.

Creating a new log harvesting profile

About this task

To create a new log harvesting profile, you must specify:

- The IP address of the server on which the product is running
- The product name
- The directories or log files
- The filter text if you have selected one or more directories

You can harvest log files for products running on different servers by specifying multiple search criteria.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, click **New**.
4. On the Create New Profile page, enter the appropriate information in the **Profile Name** and **Profile Description** fields.
5. Select the hostname of the server, product, and directories or files from the respective fields.

- To select multiple directories or files from the respective list boxes, press CTRL and click the individual directories or files.
- To clear a selection, press CTRL and click the item.
- To add another log harvesting request for another product or for another instance of the same product running on the same server or on a different server, click **+**.

6. If you select one or more directories, enter a text pattern as the filter criteria in the text box below the **Directories / Filter Text** list box field.

   During the harvesting operation, the system harvests only those files that match the filter text.

7. Click **Save Profile** to save the profile and the log harvesting requests in the profile.

Related topics:

Create New Profile field descriptions on page 784

Editing a log harvesting profile

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Edit**.
4. On the Harvest Criteria Edit page, modify the information in the **Profile Name** and **Profile Description** fields.
5. Modify the hostname of the server, product, and directories or files from the respective fields.
   - To select multiple directories or files from the respective list boxes, press CTRL and click the directories or files.
   - To clear a selection, press the CTRL and click the item you select.
   - To add another log harvesting request for another product or for another instance of the same product running on the same server or on a different server, click **+**.
6. If you select one or more directories, you can enter a new filter criteria in the text box below the **Directories / Filter Text** field and click **Commit**.

   During the harvesting operation, the system harvests only those files that match the filter text.

7. Click **Save Profile** to save the changes you made to the log harvesting profile.

Related topics:

Harvest Criteria Edit field descriptions on page 785

Viewing the harvested log files in an archive

You can view the harvested log files of a product stored in an archive file.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, select a log harvesting request from the table in the Harvest Criteria View section.
5. Click **Show files**.

   On the Search Archives page, navigate through the folders in the archive to view the harvested log files.

Deleting a profile

About this task

You cannot delete a profile that is in use by the Log Harvester service. If you attempt to delete a profile that is in use, the system displays an error message.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Delete**.
4. On the Profile Delete Confirmation page, click **Delete**.

Note:

Deleting a profile also deletes all the requests and all the archives related to it from the file system.

Submitting a request for harvesting log files

About this task

Use this feature to submit a log harvesting request to one or more products running on the same or different servers. After the request is successfully processed, the system, on which the products are installed, returns the harvested log files that are specified in the request. When you select a profile and click the **Request** button, the system generates a single request for all the requests contained in the profile.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Requests**.
4. On the Harvest Archives page, enter the relevant information in the **Archive Name** and **Archive Description** fields.

   The system saves the harvested log files in the specified archive file.
5. Click **Run Profile** to send a request.

   The table in the Harvest Criteria View section provides you the status of the log harvesting request. If the execution status of the request is successful, then the system creates a zip file containing the harvested log files and saves the file in the specified location.

Related topics:

Harvest Archives field descriptions on page 787

Viewing details of a log harvesting request

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Criteria View section.

   If the table does not display any request, you need to submit a new request.
5. Click **View**.

The Harvest - View Harvest detail page displays the details of the selected request.

Related topics:

Harvest - View Harvest detail field descriptions on page 790

Searching for text in a log file

Use this feature to search for matching text in the log file of a product.

About this task

The search is based on Lucene Search. The search results are highlighted as per the Lucene highlighter. The highlight package contains classes to provide *keyword in context* features, typically used for highlighting search terms on the results page.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, select a log harvesting request from the table in the Harvest Criteria View section.

   You must select a log harvesting request for which logs are successfully harvested.
5. On the Search Archives page, in the **Enter search text** field, enter the text that you want to search for.
6. In the Tree view, navigate to the log file by expanding the folders and select the log file.
7. Click **Search**.
   The system displays the search results in the Search Result Panel. The **Search Result Panel** field displays the line numbers as hyperlinks on which the searched text is found.
8. Click the hyperlink in the **Search Result Panel** field.
   When you click the hyperlink, the system displays the page containing the highlighted searched text in the **Log Browser Panel** field.

Related topics:

Search Archives field descriptions on page 789

Viewing the contents of harvested log files

About this task

Use this feature to view the log messages stored in the harvested log files for a product. You can view the contents of one log file at a time.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Criteria View section.

   If the system does not display any request in the table, you must submit a new request.
5. Click **Show Files**.
6. On the Search Archives page, select a harvested log file.

   If you select the product name or the hostname of a server on which a product is installed, the system displays an error message.
7. Click **Search**.

Related topics:

Search Archives field descriptions on page 789

Downloading harvested log files

About this task

Use this feature to download the harvested log files of one or more products you stored in a zip file on your local server.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Criteria View section.

   If the table does not display any request, you need to submit a new request.

5. Click **Show Files**.
6. On the Search Archives page, select a product name, hostname of the server on which one or more products are running, or a directory.
   - If you select a product name, the system creates a zip file containing the harvested log files for the selected product instances running on the same server or on different servers.
   - If you select a hostname of a server under a product, the system creates a zip file that contains the harvested log files for the products running on the server you selected.
   - If you select a directory, the system creates a zip file containing the harvested log files under the selected directory.
7. Click **Download**.

   The system prompts you to save the file on your local server.
8. Click **Save**.

Related topics:

Search Archives field descriptions on page 789

Filtering log harvesting profiles

Use this feature to set filter criteria to view only those log harvesting profiles that meet the set filter criteria. The titles of the columns of the table that displays the log harvesting profiles are the filter criteria.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, click **Filter: Enable**.

   You can find this button at the top right of the table containing log harvesting profiles.
4. Enter or select the filter criteria.

   You can filter the log harvesting profiles by the name, description and creator of the profiles.
5. Click **Filter: Apply**.

Note:

If no records matching the filter criteria are found, the Log Harvester page displays a message that no records matching the search criteria are found.

The log harvesting profile table displays the profiles that matches the specified filter criteria.

Filtering log harvesting requests

Use this feature to set filter criteria to view only those log harvesting requests that meet the set filter criteria. The titles of the columns of the table that displays the log harvesting requests are the filter criteria.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click **Filter: Enable**.

   You can find this button at the top right of the table containing the log harvesting profiles.
5. Enter or select the filter criteria.

   You can filter the log harvesting requests by:

   - The request ID of the log harvesting request. For example, to view the requests starting with Request ID 5, enter 5.
   - The zip file name that stores the harvested files.
   - The description of the log harvesting request.
   - The location of the archived file that stores the harvested files.
   - The status of the log harvesting request.
   - The description of the log harvesting request status.
6. Click **Filter: Apply**.

Note:

If no records matching the filter criteria are found, the Log Harvesting page displays a message that no records matching the search criteria are found.

The table containing log harvesting requests displays only those log harvesting requests that match the specified filter criteria.

Viewing details of a log harvesting profile

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **View**.

   The Profile Criteria View page contains the details of the log harvesting profile you selected.

Related topics:

Profile Criteria View field descriptions on page 786

Log Harvester field descriptions

This page displays the list of log harvest profiles created in System Manager. You can use buttons on this page to perform the following operations:

- View and edit the details of a selected log harvest profile.
- Delete a profile.
- Add a new log harvest profile.
- View the details of log harvest requests for a profile.

Name	Description
Profile Name	Specifies the name of the log harvesting profile.
Description	A brief description of the profile.
Created By	Specifies the name of the creator of the profile.
Created Time Stamp	Specifies the date and time when the profile was created.

Button	Description
View	Opens the Harvest Archives page. You can use this page to view the details of a selected log harvest profile.

Button	Description
New	Opens the Create New Profile page. You can use this page to create a new log harvesting profile.
Edit	Opens the Edit Profile page. You can use this page to edit a log harvesting profile.
Delete	Deletes the selected profile. You can not delete a profile if the profile is in use by the Log Harvester service.
Requests	Opens the Harvest Archives page. You can use this page to run the log harvesting requests in a selected profile.
Filter: Disable	Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays fields under the columns in the table where you can enter the filter criteria. Only columns on which you can apply filter display the fields in which you can enter the filter criteria. This is a toggle button.
Filter: Apply	Filters the log harvest profiles present in the system based on the filter criteria.

Create New Profile field descriptions

Use this page to create a new log harvesting profile for harvesting log messages from the log files for one or more products which may reside on one or more servers.

Name	Description
Profile Name	Specifies the name of the log harvesting profile.
Profile Description	Specifies a brief description of the profile. This is an optional field.
Host Name	Specifies the hostname of the servers on which products are installed.
Product	Specifies the products for which you can harvest logs.
Directories / Filter Text	Lists the directories that contains the log files for the selected product.

Name	Description
Files	Specifies the log files that you can harvest for the selected product.
Filter Text	Specifies the text based on which the log files present under a selected directory are filtered for harvesting. If you select the directory `/a/b/c` and enter the text `com` in this field, the harvest operation for this profile harvests the log files present under the directory `/a/b/c`. The log files contain com in the file name. This field does not support wild characters.

Button	Description
+	Specifies another log harvesting request for a product.
-	Deletes the log harvesting request for the product.
Commit	Commits the filter criteria for the selected directories.
Save Profile	Saves the new profile and settings for log harvesting requests in the database.

Harvest Criteria Edit field descriptions

Use this page to edit an existing log harvesting profile.

Name	Description
Profile Name	Specifies the name of the log harvesting profile
Profile Description	Specifies a brief description of the profile.
Host Name	Specifies the IP addresses of the servers on which you installed the products.
Product	Specifies the products for which you can harvest logs.
Directories / Filter Text	Lists the directories that contains the log files for the selected product.
Files	Specifies the log files that you can harvest for the selected product

Name	Description
Filter Text	Specifies the text based on which the log files present under a selected directory gets filtered for harvesting. If you select the directory `/a/b/c` and enter `com` in the **Filter Text** field, the harvest operation for this profile harvests the log files present in the directory `/a/b/c`. The log files contain com in the file name. The field does not support wild characters.

Button	Description
+	Allows you to specify another log harvesting request for a product.
-	Deletes the log harvesting request for the product.
Commit	Commits the filter criteria for the selected directories.
Save Profile	Saves the new profile and settings for log harvesting requests in the database.
Cancel	Ignores the changes you make to the Harvest Criteria Edit page and takes you back to the Log Harvester page.

Profile Criteria View field descriptions

Use this page to view the details of a selected log harvest profile.

Name	Description
Profile Name	Specifies the name of the log harvesting profile.
Profile Description	A brief description of the profile.
Product	Specifies the name of the product for which logs are harvested.
Hosts	Specifies the IP address of the server on which the product resides.
Files	Specifies the names of the log files for which you can harvest log messages.
Directory	Specifies the directory that contains the log files.

Name	Description
Filter Text	The text based on which the log files present under a selected directory are filtered for harvesting. For example, if you select the directory `/a/b/c` and enter the text `com` in this field, the harvest operation for this profile harvests the log files present under the directory `/a/b/c`. The log files contain com in the file name. This field does not support wild characters.

Button	Description
Done	Closes this page and takes you back to the Harvest Profile List page.
Refresh	Refreshes the records in the table.

Harvest Archives field descriptions

Use this page to create a archive for the log harvesting request. The archive created for a successful harvesting request contains the requested log files in a zip file. You can use the buttons on this page to perform the following operations:

- Run the log harvesting requests in a selected profile.
- View the details of the execution of a log harvesting request.
- View the log files stored in an archived file.

Name	Description
Archive Name	The name of the archive file that you want to create for storing the harvested log files.
Archive Description	A brief description of the archive. This field is optional.

Name	Description
Request Id	The unique identification number assigned to a log harvesting request.
Zip file name	The name of the zip file that contains the harvested log files.
Request Time Stamp	The date and time when the log harvesting request is submitted.
Request Description	A brief description of the log harvesting request.

Name	Description
Status	The status of the log harvesting request. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager failed to harvest the log messages for the product. • PARTIAL SUCCESS: The status is PARTIAL SUCCESS if System Manager partially harvests the log messages.
Status Time Stamp	The date and time when the execution status of the log harvesting request is generated.
Status Description	A brief description of the log harvesting request status. The description provides you the information about the success or failure of the log harvesting request.
Location	The location where the harvested log messages are archived.

Button	Description
Run Profile	Runs the log harvesting requests for the selected profile.
View	Opens the View Harvest detail page. You can use this page to view the details of a selected log harvesting request.
Show Files	Opens the Search Archives page. You can use this page to search for text contained in the harvested log files, download log files of one or more products running on a same or different servers, view the contents of a log file.
Filter: Disable	Hides the fields displayed under the column filter fields without resetting the filter criteria. A toggle button.
Filter: Enable	Displays fields under the column headers of the table displaying the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields in which you can enter the filter criteria. This is a toggle button.

Button	Description
Filter: Apply	Filters the log harvest profiles present in the system based on the filter criteria.

Search Archives field descriptions

Use this page to perform the following activities on the log files contained in an archive:

- View the contents of the harvested log files.
- Search a text in the harvested log files.
- Download the harvested log files on your local server.

Name	Description
Enter search text	The text that you want search for in the harvested log files.
List box	Displays the hierarchy of the harvested log files in an archive. The files are organized in a tree view.
Log Browser Panel	Displays the contents of the selected log files.
Search Results Panel	Displays the search results. This field displays the line numbers as hyperlinks in which the searched text is found. When you click the line number, the system displays the line containing the searched text at the top in the **Log Browser Panel** field.

Button	Description
Previous	Displays the log file contents on the previous page. This button is available only if the contents of a log files span across multiple pages.
Next	Displays the log file contents on the next page. This button is available only if the contents of a log files span across multiple pages.
Search	Searches for the occurrences of the text specified in the **Enter search text** field in the selected log files.
View	Displays the contents of the selected log files in the **Log Browser Panel** field.

Button	Description
Download	Downloads the selected log files present in the archive on your local server.

Harvest - View Harvest detail field descriptions

Use this page to view the details of a selected log harvest request.

View Parent

Name	Description
Request ID	Specifies the unique identification number assigned to a log harvesting request.
Archive	Specifies the name of the archive file that stores the harvested log files containing the log messages.
Status	Specifies the status of log harvesting requests. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager fails to harvest the log messages for the product.
Request Description	A brief description of the log harvesting request.

Harvest View

Name	Description
Product	Specifies the unique identification number assigned to a log harvesting request.
Status	Specifies the status of the log harvesting request. The options are: • **SUCCESS**: The status is SUCCESS if System Manager successfully harvests the log messages. • **FAILURE**: The status is FAILURE if System Manager fails to harvest the log messages for the product.

Name	Description
Host Name	Specifies the IP address of the server on which the product resides.
Status Description	A brief description about the execution status of the request.
Status Time Stamp	Specifies the date and time when the execution status of the log harvesting request is generated.

Button	Description
Done	Closes this page and takes you back to the Harvest Archives page.
Refresh	Refreshes the records in the table.
Filter: Enable	Displays fields under the column headers of the table displaying the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields in which you can enter the filter criteria. A toggle button.
Filter: Apply	Filters the log harvesting requests based on the filter criteria.
Filter: Disable	Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. A toggle button.

Managing log settings

Log Settings

Log Settings displays the loggers and appenders for any log configuration file that you select. You can also modify the logger and appender settings through this menu. The Logger List displays the name and level of the log along with the appender details.

Accessing the Log Settings service

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.

2. In the left navigation pane, click **Logs** > **Log Settings**.

Result

The system displays the **Log Settings** page.

Viewing loggers for a log file

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** drop-down field.
   You can view the loggers in the Logger List.

Related topics:

Logging Settings field descriptions on page 792

Logging Settings field descriptions

Use this page to view and edit loggers defined in a log file.

Log Settings

Name	Description
Select Log File	The field lists the log files that you can configure.

Logger List

Name	Description
Logger	Specifies the loggers in the selected log files.
Log level	Specifies the log level indicating the level of logging set for the corresponding logger.
Attached Appenders > Name	Specifies the name of the appender.
Attached Appenders > File Path	Specifies the path of the file to which the appender logs the information.

Name	Description
Attached Appenders >Facility	Specifies the process running on the machine that created the log message.
Attached Appenders > host	Specifies the name of the syslog host where the log output is stored.
Show All	Provides you an option to select the maximum number of logger records that you can view at a time.

Button	Description
Edit	Opens the Edit Logger page that you can use to edit loggers.

Related topics:

Viewing loggers for a log file on page 792

Editing a logger in a log file

About this task

You can set log levels for loggers which define as to what level of logging the logger logs.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, select a log file from the **Select Log File** field.
4. Click a logger in the **Logger List** section.
5. Click **Edit**.
6. On the Edit logger page, in the **Log Level** field select a log level.

Note:

As a user of System Manager Communication Manager capabilities, if you want to view the logs for successful events, then change the **Log Level** settings for any specified log to **Info**. The **Info** setting enables the system to log the successful events. When you set the **Log Level** to **Info** in `com.avaya.iptcm.eps.logging.audit` and `com.avaya.iptcm.eps.logging.operation`, the system captures the successful events in the audit log and the operational log present at `/var/log/Avaya/mgmt/iptcm/audit.log` and `/var/log/Avaya/mgmt/iptcm/operation.log` respectively. Note that if you carry out an application upgrade, the system does not retain the modified log level configuration. After an

application upgrade, you must configure the log level settings again to view the logs for successful events.

7. Click **Commit**.
   The log level is set for the selected logger.

Related topics:

Edit Logger field descriptions on page 795

Assigning an appender to a logger

About this task

The appender where a logger logs the log messages.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, select a log file from the **Select Log File** field.
4. In the Logger List section, select a logger and click **Edit**.
5. On the Edit logger page, click **Attach** in the Attached Appenders section.
6. On the Attach Appender page, select an appender in the **Select Appender** field.
7. Click **Commit**.
   The appender is added to the selected logger and you can view the appender on the **Log Settings** page.

Related topics:

Attach Appender field descriptions on page 797

Modifying an appender

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, select a log file from the **Select Log File** field.
4. In the Logger List section, select a logger and click **Edit**.
5. On the Edit logger page, select an appender in the **Attached Appenders** section.
6. Click **Edit**.
7. On the Edit Appender page, modify the appender information.

You can modify information in the **Threshold Log Level**, **Max File Size**, **File Path**, and **Number Of Backup Files** fields

8. Click **Commit**.

Related topics:

Edit Appender field descriptions on page 796

Removing an appender from a logger

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the Logger List section, select a logger and click **Edit**.
5. On the Edit logger page, select an appender in the **Attached Appenders** section.
6. Click **Detach**.

Edit Logger field descriptions

Use this page to edit logger and appender information. You can also add and remove appenders from the loggers.

Logger

Name	Description
Logger	Specifies the name of the logger.
Log level	Specifies the level of logging for which the logger logs the information.

Attached Appender

Name	Description
Appender	Specifies the name of the appender.
Threshold Log Level	Specifies the threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level.
File Path	Specifies the path of the file where the appender logs the information.
Max File Size	Specifies the maximum size in KB, MB, and GB reserved for the appender file.

Name	Description
# Backup Files	Specifies the number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created.
Facility	Specifies the process running on the machine for which log messages are created.
Host	Specifies the name of the syslog host that stores the log output.
Header	Specifies the header part of the syslog packet. The header part contains timestamp and host name information.
Facility Printing	Specifies the printed message includes the facility name of the application.

Button	Description
Edit	Opens the Edit Appender page. Use this page to modify the appender information.
Attach	Opens the Attach Appender page. Use this page to add an appender to the logger.
Detach	Removes the selected appender from the logger.
Commit	Saves the changes in the logger information to the database.
Cancel	Closes the Edit Logger page and takes you back to the Logging Configuration page.

Edit Appender field descriptions

Use this page to edit the information of an appender.

Name	Description
Logger	Specifies the name of the logger. **Note:** You can only view this information.
Appender	Specifies the name of the appender. **Note:** You can only view this information.

Name	Description
Threshold Log Level	Specifies the threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level .
File Path	Specifies the path of the file where the appender logs the information.
Max File Size	Specifies the maximum KB, MB, and GB reserved for the appender file.
# Backup Files	Specifies the number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created.

Button	Description
Commit	Saves the changes to the database.
Cancel	Closes Edit Appender page and takes you back to the Edit Logger page.

Attach Appender field descriptions

Use this page to assign an appender to the logger.

Name	Description
Logger	Specifies the name of the logger.
Log Level	Specifies the level of logging for which the logger logs the information.
Select Appender	Specifies the list of appenders that you can assign to the logger.

Button	Description
Commit	Assigns the appender to the logger.
Cancel	Closes the **Attach Appender** page and takes you back to the Edit Logger page.

Managing log viewer

Log Viewer

Log Viewer displays all the logs generated by System Manager and its adopters. The Log List displays a list of all the logs. You can view the details of each log, perform a search for logs, and filter specific logs. Log details include information about the event which generated the log, the severity level of the log, and other relevant information. You can search logs based on search conditions and set filters to view logs that match the filter criteria. Log viewer displays only logs that are of type Audit.

Viewing log details

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
3. On the Logging page, select a log.
4. Click **View**.

Searching for logs

Use the advanced search function to find logs based on certain specified conditions. The system displays only those logs that satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
3. On the Logging page, click **Advanced Search**.
4. In the **Criteria** section, from the first and second drop-down fields, select the search criterion and the operator.
5. Select or enter the search value in the third field.
6. If you want to add another search condition, click **+** and repeat the steps 4 through 6.

Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.

7. Select the **AND** or **OR** operator from the drop-down field.

   This page displays this drop-down field when you specify more than one search condition.

8. Click **Search** to find the logs for the given search conditions.

Filtering logs

You can filter and view logs that meet the specified filter criteria. To apply the filters, you need to specify the filter criteria in the fields provided under select columns in the table displaying the logs. The column titles are the filter criteria. You can filter logs on multiple filter criteria.

Procedure

1. On the System Manager Web Console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
3. On the Logging page, click **Filter: Enable** at the top right corner of the log table.
4. Enter or select the filter criteria.
5. Click **Filter: Apply**.

   The page displays the logs that match the specified filter criteria.

   Note:

   If no records matching the filter criteria are found, the Management Console application displays a message that no records matching the search criteria are found.

Logging field descriptions

The Logging page has two sections: the upper section contains buttons that allow you to view the details of the selected logs, search for logs, and set filters. The lower section displays logs in a table. The table provides information about the logs. You can click the title of the column to sort the data of the column in ascending or descending order.

Name	Description
Select check box	Provides the option to select a log.

Name	Description
Log ID	Specifies the unique identification number that identifies the log.
Time Stamp	The date and time of the log generation.
Host Name	Specifies the name of the system from which the log is generated.
Product Type	Specifies the code which uniquely identifies the component which generated the log. For example, product, device, application, and service. An example of the log product type is GW600, which is a product type code identifier.
Severity	Specifies the severity level of the log. The following are the type of severities: • **Emergency**: System is unusable. • **Alert**: Action must be taken immediately. • **Critical**: Critical conditions. • **Error**: Error conditions. • **Warning**: Warning conditions. • **Notice**: Normal but significant condition. • **Informational**: Informational messages. • **Debug**: Debug-level messages. **Note:** The colors of severities do not indicate logging severities.
Event ID	Specifies the unique identification number assigned to the event that generated the log.
Message	A brief description about the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.
Process Name	The process on the device that has generated the message, usually the process name and process ID.
Facility	The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated

Name	Description
	them, along with the severity of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
View	Opens the Log - View Log Detail page. Use this page to view the details of the selected log.
Auto-Refresh Mode	Switches to the Auto-Refresh mode. When the Logging page is set in this mode, it automatically updates the logs in the table. A toggle button.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a log.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. A toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. A toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters logs based on the filter criteria.
Select: All	Selects all the logs in the table.
Select: None	Clears the selections.
Previous	Displays logs in the previous page. This button is not available if you are on the first page.
Next	Displays logs in the next page. This button is not available if you are on the last page.

Criteria section

This section appears when you click **Advanced Search** on the top right corner.

Name	Description
Criteria	Use this section to specify search conditions. Select the search criteria from the first drop-down field. Select the operator from the

Name	Description
	second drop-down list. Enter the search value in the text field. Select following search criteria from the first drop-down list: • Log ID: The unique identification number assigned to the log. • Host Name: Name of the system for which log is generated. • Product type: A code which uniquely identifies the component which generated the log. For example, product, device, application, service, and so on. • Severity: Severity level of the log. • Message: Brief description about the log. • Event ID: Unique identification number assigned to the event. • Process Name: Process on the device that has generated the message • Time Stamp: Date and time of the log generation. • Facility: The operating systems, processes, and applications quantify messages into one of several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The second drop-down list displays operators. Based on the search criterion that you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down list. The following are the list of operators: • Equals • Not Equals • Starts With • Ends With • Contains The operators for Time Stamp are: =, >, <, >=, <=, and !=. When you select Time Stamp from the first drop-down list, the page provides date and

Name	Description
	time fields for entering the date and time in the respective fields. Enter the date in MM/DD/YYYY format . You can select the date from the calender. You need to enter the time in one of the following formats: • 24Hr • AM • PM

Button	Description
Clear	Clears the search criterion and sets the criterion to the default search criteria.
Search	Searches the logs based on the search conditions.
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	Deletes a search condition

Logging field descriptions

Use this page to view logs in the Auto-Refresh mode. In this mode, the page updates the log information automatically.

Name	Description
Log ID	Specifies the unique identification number that identifies the log.
Time Stamp	Specifies the date and time of the log generation.
Host Name	Specifies the name of the system from which the log is generated.
Product Type	Specifies the code which uniquely identifies the component which generated the log. For example, product, device, application, service and so on. GW600, which is a product type code identifier is an example of the log product type.
Severity	Specifies the severity level of the log. The following are the type of severities:

Name	Description
	• **Emergency**: System is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant condition • **Informational**: Informational messages • **Debug**: Debug-level messages **Note:** The colors of severities do not indicate logging severities.
Event ID	Specifies the unique identification number assigned to the event that has generated the log.
Message	Brief description about the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.
Process Name	Specifies the process on the device that has generated the message. This is usually the process name and process ID.
Facility	The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
Logging Landing Page	Switches the mode from Auto-Refresh to manual refresh and displays the Logging Home page. This is a toggle button.

TrapListener service

The TrapListener service receives traps and informs coming from different applications and displays them on the System Manager Alarming UI.

- TrapListener receives V2c and V3 traps and informs that are defined in the common alarm definition file.
- Traplistener also processes the Common Alarm Definition file for applications, where all the trap definitions are present.

You can configure the trap listener service through Service Profile Management. For information on configuring the TrapListener service, see Configuring the TrapListener service on page 756.

If you change the Trap Listener settings, as an administrator you should create a new SNMP Target profile for the System Manager IP address, and a new SNMPv3 user profile for the System Manager. The values in these profiles should match the values in the Trap Listener settings. You should also attach this SMGR SNMPv3 user profile to the SMGR Target profile, and then attach this Target profile to all the Serviceability Agents. For information on creating SNMP User and Target profiles and attaching the Target profiles to Serviceability Agents, see *Chapter 6, Managing Serviceability Agents in the Administering Avaya Aura System Manager guide Release 6.2*.

SystemMonitor service

About SystemMonitor service

The SystemMonitor service runs on the System Manager server as a Linux service and periodically monitors the PermGen, physical memory (RAM), CPU, hard disk usage, heap memory, and operating system swap space. The SystemMonitor service raises alarms when the monitored items reach their threshold values. The threshold values are expressed in percentage.

The system clears the alarm when the monitored item reaches the warning threshold. View the SystemMonitor alarms on the System Manager Web Console.

Related topics:

Threshold values for the system properties on page 806

Modifying the threshold value for system properties

You can define the threshold values for system configuration properties in the `MonitorConfig.properties` file.

Procedure

1. To view the SystemMonitor alarms:

   On the System Manager Web Console, click **Services** > **Events**.

   a. In the left navigation pane, click **Events** > **Alarms**.
   b. On the Alarming page, select an alarm from the Alarm List. You can select multiple alarms.
   c. Click **View**.
   The system displays the alarm details on the Alarm - View Alarm Detail page.

2. Navigate to the `$MGMT_HOME/SystemMonitor/res` directory for the configuration properties file.
3. Modify the threshold values in the `MonitorConfig.properties` file and save the file.

   For threshold value for a system property, see Threshold values for the system properties on page 806. For the changes to take effect, restart the SystemMonitor service.

4. To restart the SystemMonitor service, at the command prompt, type `service systemMonitor restart`.

Related topics:

Threshold values for the system properties on page 806

Threshold values for the system properties

The properties and their default threshold values of SystemMonitor are as follows:

Table 8: Threshold values

Property	Threshold value	Alarm description
PhysicalMemoryMonitor.CriticalThreshold	90	PhysicalMemoryMonitor reached critical level

Property	Threshold value	Alarm description
PhysicalMemoryMonitor.WarningThreshold	70	PhysicalMemoryMonitor reached warning level
CPUMonitor.CriticalThreshold	95	CPUMonitor reached critical level
CPUMonitor.WarningThreshold	80	CPUMonitor reached warning level
DiskMonitor.CriticalThreshold	90	DiskMonitor reached critical level
DiskMonitor.WarningThreshold	75	DiskMonitor reached warning level
HeapMonitor.CriticalThreshold	90	HeapMonitor reached critical level
HeapMonitor.WarningThreshold	60	HeapMonitor reached warning level
SwapSpaceMonitor.CriticalThreshold	90	SwapSpaceMonitor reached critical level
SwapSpaceMonitor.WarningThreshold	70	SwapSpaceMonitor reached warning level

Chapter 10: Managing licenses

WebLM overview

Log on to the System Manager Web Console.

Avaya provides a Web-based license manager (WebLM) to manage licenses of one or more Avaya software products for your organization. WebLM is a Web-based license manager that facilitates easy tracking of licenses. To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) Web site at https://plds.avaya.com.

The license file of a software product is in an XML format. The license file contains information regarding the product, the major release, the licensed features of the product, and the licensed capacities of each feature that you purchase. After you purchase a licensed Avaya software product, you must activate the license file for the product in PLDS and install the license file on the WebLM server.

License activations in PLDS require the host ID of the WebLM server for inclusion in the license file. The host ID of the WebLM server is displayed on the Server Properties page of the WebLM server .

Obtaining the license file

About this task

Obtain a license file from PLDS to install on the WebLM server for each licensed Avaya product that you require to manage from the WebLM server. For additional information on using PLDS, see *Getting Started with Avaya PLDS - Avaya Partners and Customers* at https://plds.avaya.com.

⚠ Caution:

Do not modify the license file that you receive from Avaya. WebLM does not accept a modified license file.

You need the host ID of the WebLM server to activate the license file in PLDS.

Procedure

1. Log on to the System Manager Web Console.
2. On the System Manager Web Console, click **Services** > **Licenses**.
3. In the left navigation pane, click **Server properties**.
4. Note the **Primary Host ID**.

   Though Avaya recommends the use of the primary host ID, you can use any of the host IDs that the Server Properties page lists.

Accessing WebLM

Before you begin

You must have permissions to access the WebLM application.

Procedure

1. Log on to the System Manager Web Console.
2. On the System Manager Web Console, click **Services** > **Licenses**.

Installing a license file

Use this functionality to install a license file on the WebLM server. If you are reinstalling a license file on a WebLM server on which the license file that Remote Feature Activation (RFA) generated is installed, you must remove the license file that RFA generated from the WebLM server before you install the new license file. Use the Uninstall functionality to remove the license file from the WebLM server.

Before you begin

- Obtain the license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.
- Log on to WebLM Home.

About this task

If you experience problems while installing the license file, see the License file installation errors section in *Administering Avaya WebLM (stand-alone)*.

Procedure

1. In the left navigation pane, click **Install license**.
2. On the Install license page, enter the license file path. You can also click **Browse** to select the license file.
3. Click **Install** to install the license file.
   WebLM displays a message upon successful installation of the license file. The installation of the license file can fail for various reasons, such as:
   - WebLM finds an invalid digital signature on the license file. If you get such an error, request PLDS to redeliver the license file.
   - The current capacity use exceeds the capacity in the installed license.

Related topics:

Obtaining the license file on page 809
Install license field descriptions on page 814

Viewing the license capacity of the product features

Use this functionality to view the license capacity of the features of a product for which you installed a standard license file.

Before you begin

- Log on to WebLM Home.
- Install the standard license file on the WebLM server for the licensed product.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **View license capacity**.
   The content pane displays the capacity of the licensed features of the product.

Related topics:

View license capacity field descriptions on page 814

Viewing peak usage for a licensed product

Before you begin

- Log on to WebLM Home.
- Install the standard license file on the WebLM server for the licensed product.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **View peak usage**.

Related topics:

View peak usage field descriptions on page 815

Removing a license file

Use this functionality to remove the license file that you install on the WebLM server.

Before you begin

Log on to WebLM Home.

Procedure

1. In the left navigation pane, click **Uninstall license**.
2. On the Uninstall License page, select the license file that you require to delete.
3. To remove the license file from the WebLM server, click **Uninstall**.

Related topics:

Uninstall license field descriptions on page 816

Viewing the server properties

Before you begin

Log on to WebLM Home.

Procedure

In the left navigation pane, click **Server properties**.

The Server Properties page displays the host ID. The host ID is the MAC address of the computer on which you installed WebLM.

Note:

The host ID specified in PLDS is embedded in the license file. You can install the license file only if the host ID of the target computer matches the host ID in the license file. Therefore, when you request for a license file, specify the correct host ID of the computer where the WebLM server is installed.

Related topics:

Server Properties field descriptions on page 817

WebLM Home field descriptions

Use this page to view the information about the product(s) and the associated license file(s) installed on the WebLM server.

Field	Description
Product Name	The name of the product for which the license file is installed.
Product Version	The version of the product for which the license file is installed.
Type of License	The type of license file installed for the product.
Date of Installation	Date and time of installation of license file.

Install license field descriptions

Use this page to install the license file of a product on the WebLM server.

Field/Button	Description
Enter license path	Specify the complete path where you saved the license file.
Browse	Opens the dialog box using which you can select the license file.
Install	Installs the product license file.

View license capacity field descriptions

Use this page to view the total number of feature licenses of a product that the organization has purchased and the current allocation of these purchased licenses.

Field	Description
Feature (Keyword)	The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.
Expiration Date	The date on which the license for the feature expires. The date on which the feature license expires.
Licensed	The number of feature licenses purchased by the organization for each licensed feature. The system gathers the number of feature licenses information from the license file.
Acquired	The number of feature licenses that are currently in use by the licensed application. For features of type Uncounted, the column displays *Not counted*.

The Acquired licenses table displays information about the licenses acquired by the licensed application. You can view this table only if the licensed product has acquired feature licenses.

Field	Description
Feature	The feature keyword for each licensed feature that is currently acquired by a licensed application.
Acquired by	The name of the licensed application that has acquired the license.
Count	The number of feature licenses that are currently acquired by the licensed application.

Related topics:

Viewing the license capacity of the product features on page 811

View peak usage field descriptions

Use this page to view the usage information of feature licenses of a licensed application for different time intervals.

Field	Description
Feature (License Keyword)	The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.
Currently allocated	The number of feature licenses purchased by the organization.
Usage: qty/%	The number of feature licenses for each licensed feature that a licensed application currently uses. The column also displays the percentage of usage. For example, if 50 feature licenses are available and five feature licenses are used by applications, the column displays 5/10%.
Peak usage (last 7 days): qty/%	The highest number of feature licenses for each licensed feature that has been used in the last seven days. For example, if the peak usage for a feature license in the past seven days was 25, and the number of available licenses during these seven days was 50, then the column displays 25/50%.

Field	Description
Peak usage (last 30 days): qty/%	The highest number of feature licenses for each licensed feature that has been used in the past 30 days. For example, if the peak usage for a feature license in the past 30 days was 50, and the number of available licenses during these 30 days was 50, then the column displays 50/100%.
Time of query	The date and time when the last usage query for WebLM was executed.
Status	The success or failure of the last usage query executed for the WebLM server.

Related topics:

Viewing peak usage for a licensed product on page 812

Uninstall license field descriptions

Use this page to remove a license file from the WebLM server for a licensed product.

Field	Description
Installed license file	The name of the license files currently installed on the WebLM server.
Products	The products for which licenses are installed on the WebLM server.
SID	The System ID of the license file.
Select Check box	Use to select the license files that you require to remove from the WebLM server.

Button	Description
Uninstall	Removes the selected license files from the WebLM server.

Related topics:

Removing a license file on page 812

Server Properties field descriptions

Use this page to view the MAC address of the server.

Server Host ID

Field	Description
Primary Host ID	Displays the MAC address of the server. You can assign more than one MAC address to the server. The first MAC address is the primary MAC address and subsequent MAC addresses are designated as secondary MAC address, tertiary secondary MAC address. Use the primary MAC address in the license file. **Note:** In a Solaris server, where the MAC address is not available, for example, in a zoned environment, WebLM retrieves the 8–digit hexadecimal host ID of the server and adds leading zeros to make the ID a 12–digit address.

Usage history count

Field/Button	Description
Count	Specifies the number of usage query results that the server maintains.
Submit	Commits the changes you made to the Server Properties page.
Cancel	Discards the changes you made to the Server Properties page.

Related topics:

Viewing the server properties on page 813

Enterprise licensing

Configuring enterprise licensing

Before you begin

- Log on to WebLM Home.
- Install the enterprise license file on the WebLM server for the product.

  To verify the type of the license file for a product, in the left navigation pane, click **Licensed products** and select the product name. The content pane displays the product name, System Identification number (SID), and the license file type installed for the product at the top of the page.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. In the left navigation pane, click **Enterprise configuration**.
3. On the Enterprise Configuration page, enter the appropriate information in the fields.

   For a detailed information of the fields, see Enterprise Usage field descriptions on page 838.

   To successfully set up and configure the master WebLM server, enter valid information in the mandatory fields that are marked with a red asterisk.
4. In the **Master WebLM Configuration** section, enter the name, description, and IP address of the master WebLM server.
5. In the **Default Periodic Operation Settings** section, enter the retry count and the retry interval in minutes for the periodic operations.
6. In the **SMTP Server settings** section, enter the name of the SMTP server.
7. In the **E-mail notification settings for periodic operation** section, perform the following:
   a. Set the **E-mail notification** to On.
   b. In the **E-mail address** field, enter an e-mail address.
   c. To add the e-mail address to the list of recipients for the WebLM server to send e-mail notifications, click **Add To List**.
8. In the **Default Periodic License Allocation Schedule** section, select the day and time for periodic license allocations.

The values you enter in this section remain as the default setting for periodic allocation for all local WebLM servers in the enterprise.

9. In the **Default Periodic Usage Query Schedule** section, select the day and time of the query for periodic usage.

   The values you enter in this section remain as the default setting for periodic usage for all local WebLM servers in the enterprise.

   Note:

   For any periodic operations, you must perform the manual allocation at least once.

10. Click **Submit**.
    The system validates the information. The system displays the host ID in the **MAC ID** field. The host ID is the host ID of the computer where you installed the WebLM server.

Related topics:

Enterprise Configuration field descriptions on page 828

Adding a local WebLM server

Before you begin

- Log on to WebLM Home.
- Install the enterprise license file.
- Identify the WebLM servers that you require to add as the local WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Local WebLM Configuration** > **Add local WebLM**.
3. On the Local WebLM Configuration: Add local WebLM page, enter the appropriate information.

   To successfully set up and configure the local WebLM server, enter valid information in the mandatory fields that are marked with a red asterisk (*).

   For detailed descriptions of the fields, see Add local WebLM field descriptions on page 831.
4. In the **Local WebLM Configuration** section, enter the name, description, IP address, and port of the local WebLM server. Select a protocol for the master WebLM server to communicate with the local WebLM server.

5. In the **Periodic license allocation schedule** section, select the day and time for periodic license allocations.
6. In the **Periodic usage query schedule** section, select the day and time of the query for periodic usage.
7. Click **Configure and validate**.
   The system validates the information. If the information is valid, the system displays the host ID of the computer where the server is installed in the **MAC ID** field.

Related topics:

Add local WebLM field descriptions on page 831

Modifying a local WebLM server configuration

Before you begin

- Log on to WebLM Home.
- Install the enterprise license file.
- Add at least one local WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Local WebLM Configuration** > **Modify local WebLM**.
3. On the Local WebLM Configuration: Modify local WebLM page, select the local WebLM server that you require to configure.
4. Click **Modify**.
   The system displays another Local WebLM Configuration: Modify local WebLM page with a different set of WebLM configuration fields.
5. Modify the information in the following fields:
   - In the **Local WebLM configuration** section, **Name**, **Description**, **Protocol**, and **Port**
   - In the **Periodic License Allocation schedule** section, **Day** and **Time**
   - In the **Periodic Usage Query schedule** section, **Day** and **Time**
6. Click **Modify**.
   The system saves your changes.

Related topics:

Modify local WebLM field descriptions on page 833

Removing a local WebLM server

Before you begin

- Log on to WebLM Home.
- Install the enterprise license file.
- Add at least one local WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Local WebLM Configuration** > **Delete local WebLM**.
3. On the Local WebLM Configuration: Delete local WebLM page, select the local WebLM server that you require to delete.
4. Click **Delete**.

   Note:

   The system displays a warning message before removing the local WebLM server from the master WebLM server.

5. Click **OK**.

Related topics:

Delete local WebLM field descriptions on page 835

Viewing the license capacity of the licensed features of a product

Before you begin

Log on to WebLM Home.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **View by feature**.

Related topics:

View by feature field descriptions on page 827

Viewing the connectivity status of the local WebLM servers

Before you begin

Log on to WebLM Home.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **View by local WebLM**.

   The page displays the connectivity status of the local WebLM servers.

Related topics:

View by local WebLM field descriptions on page 827

Validating connectivity to local WebLM servers for a product

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Local WebLM Configuration**.
3. On the Local WebLM Configuration: View local WebLM page, select the local WebLM servers that you want to validate for connectivity.
4. To query the selected local WebLM servers, click **Validate Connectivity**.

Result

The **status** column on the Local WebLM Configuration: View local WebLM page of the selected WebLM servers displays if the connection request made to the local WebLM server is successful.

Related topics:

View Local WebLMs field descriptions on page 830

Viewing usage by WebLM

Before you begin

Log on to WebLM Home.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Usages** > **Usage by WebLM**.
   The system displays the Usages: Usage by WebLM page.
3. In the **Select WebLM** field, select the master or local WebLM server.
4. Click **Query System**.

Related topics:

Usage by WebLM field descriptions on page 836

Viewing enterprise usage of a license feature

Before you begin

Log on to WebLM Home.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Usages** > **Enterprise Usage**.
   The system displays the Usages: Enterprise Usage page.
3. In the **Select Feature (License Keyword)** field, select the licensed feature.

   The page displays the usage of the licensed feature for the master WebLM server and the local WebLM servers.

Related topics:

Enterprise Usage field descriptions on page 838

Viewing the periodic status of the master and local WebLM servers

Before you begin

Log on to WebLM Home.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Periodic status**.
   The system displays the Periodic Status page.

Related topics:

Periodic Status field descriptions on page 843

Specifying overuse limit for licensed features

Procedure

1. On the System Manager Web Console, click **Services** > **Licenses**.
2. In the left navigation pane, click **Licensed products** and select the product name.
3. Click **Overuse**.
4. On the Overuse page, in the **update percent overuse value** field , select the percent overuse value.
5. To set the overuse limit, click **Submit**.

Related topics:

Overuse field descriptions on page 844

Querying usage of feature licenses for master and local WebLM servers

Before you begin

Log on to WebLM Home.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Usages** > **Query Usage**.
   The system displays the Usages: Query Usage page.
3. To view the usage details by feature licenses of a server, select the master or local WebLM server.
4. Click **Query Usage**.

   If you select all WebLM severs or click **Check All** and click **Query usage**, the system displays the progress of the query request.

Result

If you select one local WebLM server, the Usages: Usage by WebLM page displays the details of the local WebLM server you selected.

Related topics:

Query Usage field descriptions on page 839

Changing allocations of licensed features for a local WebLM server

Use this functionality to change the license allocations of a feature that resides on a local WebLM server for the product.

Procedure

1. Log in to the master WebLM server.
2. In the left navigation pane, click **Licensed products** and select the product name.
3. Click **Allocations** > **Change allocations**.
   The system displays the Allocations: Change Allocations page.
4. In the **New Allocation** column, enter the number of licenses you require to allocate for the feature that resides on a local WebLM server.
5. Click **Submit Allocations**.

Related topics:

Change Allocations field descriptions on page 842

Viewing allocations by features

Before you begin

Log on to WebLM Home.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Allocations** > **View by feature**.
   The system displays the Allocations: View by Feature page.

Related topics:

Allocations by Features field descriptions on page 840

Viewing allocations by the local WebLM server

Before you begin

Log on to WebLM Home.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Allocations** > **View by local WebLM**.
   The system displays the Allocations: View by Local WebLM page.
3. In the **Select Local WebLM** field, select the local WebLM server.

Result

The page displays the allocation details for the local WebLM server you select.

Related topics:

Allocations by Local WebLM field descriptions on page 841

Viewing usage summary

Before you begin

Log on to WebLM Home.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Usages**.
   The system displays the Usage Summary page.

Related topics:

Usage Summary field descriptions on page 835

View by feature field descriptions

Use this page to view the license capacity for each feature license of a product.

Name	Description
Feature (License Keyword)	The display name and the keyword for the licensed features of the product.
License Capacity	The total number of feature licenses that the organization purchases for each feature.
Currently available	The number of floating licenses of each feature that is currently available with the master WebLM server. The feature licenses that are not allocated to any local WebLM server are known as floating licenses. **Note:** For uncounted features, this column displays “Not counted”.

Related topics:

Viewing the license capacity of the licensed features of a product on page 821

View by local WebLM field descriptions

Use this page to view the information related to local WebLM servers of a product.

Name	Description
Local WebLM name	Specifies the name of the local WebLM server.

Name	Description
IP address	Specifies the IP address of the local WebLM server.
Last contacted	Specifies the date and time when the local WebLM server was last contacted.
Status	Lists the success or failure of the last connection request to each local WebLM server.

Related topics:

Viewing the connectivity status of the local WebLM servers on page 822

Enterprise Configuration field descriptions

Use this page to specify the master WebLM server settings and the default settings for the periodic operations of the server. The settings you specify in the Enterprise Configuration Web page applies to the entire enterprise unless you override the setting while you add a local WebLM.

The master WebLM server uses the settings of the periodic operations to query itself and generate the usage report for licenses.

Master WebLM Configuration

Name	Description
Name	Specifies the name of the WebLM server.
Description	Provides a brief description of the server.
IP address	Specifies the IP address of the WebLM server.
MAC ID	Specifies the host ID of the computer where you installed the WebLM server. You cannot edit the **MAC ID** field.

Default periodic operation settings

Name	Description
Retry count	Specifies the number of times a master WebLM server must try to connect to a local WebLM server for a periodic operation after a connection failure. For example, set the count to 2. The master WebLM server makes an initial unsuccessful attempt to connect to a local WebLM server.

Name	Description
	The master WebLM server makes two more attempts to connect to the local WebLM server.
Retry interval	Specifies the duration in minutes, within which the retry count specified in the **Retry count** field must be carried out. For example, suppose the **Retry count** is 2 and the Retry interval is 10 minutes. If the attempt to connect to the server fails, the master WebLM server makes two attempts in 10 minutes to connect to the local WebLM server.

SMTP Server Settings

Name	Description
Server name	Specifies the name of the SMTP server.

E-mail notification settings for periodic operation

Name	Description
E-mail notification	Specifies the e-mail notification. The notification options are: • On: Sends an e-mail notification to the administrator if the periodic operations fail. • Off: Does not send an e-mail notification to the administrator if the periodic operations fail.
E-mail address	Specifies the e-mail address to which the WebLM application sends the e-mail notification if the periodic operations fail to execute. **Note:** Click **Add To List** to add the e-mail address in the list of recipients who must receive the e-mail notification of the periodic operation status.
E-mail addresses	Provides the list of e-mail addresses to which the WebLM application sends the e-mail notifications.

Name	Description
Add To List	Adds the e-mail address that you enter in the **E-mail address** field to the list of recipients who must receive the e-mail notification of the periodic operation status.
Remove Selected	Removes the selected e-mail address from the **E-mail addresses** field.

Default Periodic License Allocation Schedule

Name	Description
Day	The day of the week on which the master WebLM server must send the ALF (Allocation license file) again to the local WebLM server.
Time	The time of the day specified in the **Day** field when master WebLM must send the ALF again to the local WebLM server.

Default Periodic Usage Query Schedule

Name	Description
Day	The day of the week on which the master WebLM server must query local WebLM servers for usage reports.
Time	The time of the day you specify in the **Day** field when the master WebLM server must query local WebLM servers for usage reports.

Button	Description
Submit	Saves the enterprise configuration.
Reset	Resets the values in the fields to the values you previously saved.

Related topics:

Configuring enterprise licensing on page 818

View Local WebLMs field descriptions

Use this page to validate the local WebLM server connection. To validate the connection, the master WebLM server tries to connect to the specified local WebLM server.

Note:

To validate the connectivity of a local WebLM server, the local WebLM server must be already added for the product.

Name	Description
Local WebLM Name	The name of the local WebLM server.
IP Address	IP address of the local WebLM server.
Last Contacted	Date and time when the local WebLM server was last contacted.
Status	Lists the success or failure of the last connection request to each local WebLM server.

Button	Description
Validate Connectivity	Validates the connectivity of the selected WebLM server.
Check All	Selects all the local WebLM server.
Clear All	Clears the selections of local WebLM servers.

Related topics:

Validating connectivity to local WebLM servers for a product on page 822

Add local WebLM field descriptions

Use this page to add a local WebLM server.

Local WebLM configuration

Name	Description
Name	Specifies the name of the server.
Description	Provides a brief description of the server.
IP Address	Specifies a unique IP address of the server. If you enter an IP address of a server that is already configured for a local WebLM server, the system displays the message: `IP Address is being duplicated`.

Name	Description
Protocol	Specifies the protocol scheme over which the master WebLM server communicates with the local WebLM server.
Port	Specifies the port number on which the master WebLM server communicates to the local WebLM server in the specified protocol scheme.
MAC ID	Specifies the host ID of the computer on which you installed the server. You cannot edit the **MAC ID** field.

Periodic License Allocation schedule

Name	Description
Day	Specifies the day of the week on which the master WebLM server must send the ALFs again to the local WebLM server. By default, the system displays the settings specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.
Time	Specifies the time of the day specified in the **Day** field when the master WebLM server must send the ALFs again to the local WebLM server. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.

Periodic Usage Query schedule

Name	Description
Day	Specifies the day of the week on which the master WebLM server must query local WebLM servers for usage reports. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the

Name	Description
	Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.
Time	Specifies the time of the day specified in the **Day** field when the master WebLM server must query local WebLM servers for usage reports. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.

Button	Description
Configure and validate	Configures the local WebLM server and validates the creation of the local WebLM server.
Back	Navigates back to View local WebLMs.

Related topics:

Adding a local WebLM server on page 819

Modify local WebLM field descriptions

Use this page to modify the information of a local WebLM server.

Local WebLM configuration

Name	Description
Name	Specifies the name of the server.
Description	Displays a brief description of the server.
IP Address	Specifies the IP address of the server. **Note:** You cannot modify the information in the **IP address** field.
Protocol	Specifies the protocol scheme over which the master WebLM server listens to the local WebLM server.

Name	Description
Port	Specifies the port number on which the master WebLM server listens to the local WebLM server in the specified protocol scheme.
MAC ID	Specifies the host ID of the computer where you installed the server. **Note:** You cannot modify the information in the **MAC ID** field.

Periodic License Allocation schedule

Name	Description
Day	Specifies the day of the week on which the master WebLM server must send the ALFs again to the local WebLM server.
Time	Specifies the time of the day you entered in the **Day** field when the master WebLM server must send the ALFs again to the local WebLM server.

Periodic Usage Query schedule

Name	Description
Day	Specifies the day of the week on which the master WebLM server must query the local WebLM servers for usage reports.
Time	Specifies the time of the day you entered in the **Day** field when the master WebLM server must query the local WebLM servers for usage reports.

Button	Description
Modify	Navigates to the Modify Local WebLM page for the local WebLM server you select.
Back	Discards the configuration changes and takes you back to the Modify local WebLM page.

Related topics:

Modifying a local WebLM server configuration on page 820

Delete local WebLM field descriptions

Use this page to delete a local WebLM server.

Name	Description
Local WebLM name	The name of the local WebLM server.
IP address	The IP Address of the local WebLM server.
check box	Use to select the local WebLM servers that you require to delete.

Button	Description
Delete	Removes the local WebLM server you selected.
Reset	Clears the selection of the local WebLM servers.

Deletion of the local WebLM server

Use the Delete Local WebLM option to delete the instance of a local WebLM server from the master WebLM server. When you delete a local WebLM server using the Delete Local WebLM option, the system does not remove the server physically. The master WebLM server sends a delete request to the local WebLM server. On receiving a delete request, the local WebLM server deletes the ALF of the product that is installed on the local WebLM server. The system deletes the instance of the local WebLM server from the master WebLM server, irrespective of the success or failure of the ALF deletion process on the local WebLM server.

If the master WebLM server is unable to send the delete request to the local WebLM server, the system deletes the instance of the local WebLM server from the master WebLM server. The ALF installed on the local WebLM server automatically expires after 30 days.

Related topics:

Delete local WebLM field descriptions on page 835

Usage Summary field descriptions

Use this page to view the usage summary for a master WebLM server, a local WebLM server, or all the WebLM servers of the product.

Name	Description
WebLM Name	Displays the names of the master WebLM server and local WebLM servers of the product.
IP address	Specifies the IP address of the master WebLM server and local WebLM servers of the product.
Time of Query	Specifies the date and time when the system executed the last usage query for the WebLM server. If the status of the last usage query is `Failed`, this column also displays the date and time of the usage query that was last successful.
Status	Specifies the success or failure status of the last usage query that the system executed for each WebLM server. The **Status** column of a WebLM server remains blank if the server is not queried even once for feature license usage. The usage query can be a periodic usage query or a nonperiodic usage query.

Related topics:

Viewing usage summary on page 826

Usage by WebLM field descriptions

Use this page to query the feature license usage by the master and local WebLM servers.

Name	Description
Select WebLM	The master and local WebLM servers for which you can view the usage.
Feature (License Keyword)	The name and keyword of the counted features of the product.
Currently Allocated	The number of feature licenses for each feature that the system currently allocates to the selected WebLM server. For the master WebLM server of the product, this column lists the floating licenses available with the server.
Usage: qty/%	The number of feature licenses for each feature that the licensed applications

Name	Description
	currently use from the allocated feature licenses. The column also displays the percentage of usage. For example, if 50 feature licenses are allocated and applications use five feature licenses, this column displays 5/10%.
Peak Usage (last 7 days): qty/%	The highest number of feature licenses for each feature that the applications use in the past seven days. The column also displays the percentage of peak usage. For example, if the peak usage in the past seven days was 25 and 50 feature licenses were available during the peak usage calculation, the column displays 25/50%.
Peak Usage (last 30 days): qty/%	The highest number of feature licenses for each feature that the applications use in the past 30 days. The column also displays the percentage of peak usage. For example, if the peak usage in the past 30 days was 50 and 50 feature licenses were available during the peak usage calculation, the column displays 50/100%.
Time of Query	The date and time when the system executed the usage query for the WebLM server you select.
Status	The success or failure of the last usage query process executed for each WebLM server. The **Status** column remains blank if the server is queried even once for feature license usage. The usage query can be a periodic usage query or a nonperiodic usage query.

Button	Description
Query System	Queries the selected WebLM server for the feature license usage.

Related topics:

Viewing usage by WebLM on page 823

Enterprise Usage field descriptions

Use this page to view the feature license usage of all WebLM servers for the selected feature.

Name	Description
Select Feature (License Keyword)	Specifies the license features for which you can view the license usage.
License capacity	Specifies the total number of feature licenses the organization purchases for each feature.
Available	Lists the number of licenses currently available with the master WebLM server.
WebLM Name	Specifies the names of the WebLM servers of the product.
Currently Allocated	Specifies the number of feature licenses that the system currently allocates to the WebLM servers for the selected feature.
Usage qty/%	Specifies the number of feature licenses that the licensed applications currently use, from the allocated feature licenses for the selected feature. The column also displays the percentage of usage. For example, if 50 is the allocated feature licenses and 5 feature licenses have been used by the applications, this column displays 5/10%.
Peak Usage (last 7 days): qty/%	Specifies the highest number of feature licenses that applications use in the past seven days for the selected feature. The column also displays the percentage of peak usage. For example, if the peak usage in the past seven days is 25 and the feature licenses those were available during the peak usage calculation is 50, the column displays 25/50%.
Peak Usage (last 30 days): qty/%	Specifies the highest number of feature licenses that applications use in the past 30 days for the selected feature. The column also displays the percentage of peak usage. For example, if the peak usage in the past 30 days is 50 and the feature licenses those were available during the peak usage

Name	Description
	calculation is 50, the column displays 50/100%.
Time of Query	Specifies the date and time when the system executes the usage query for the selected feature.
Status	Specifies the status of the last usage query process that the system executes for each WebLM server. The status can be *Success* or *Failure*.

Related topics:

[Viewing enterprise usage of a license feature](#) on page 823

Query Usage field descriptions

Use this page to query the master WebLM server, a local WebLM server, or all the WebLM servers of the product for the feature license usage report.

Name	Description
WebLM Name	The names of the master and the local WebLM servers of the product as links. To view the feature license usage of a server, select the name of the required server in the **WebLM Name** column. **Note:** If the specified WebLM server is not queried even once for feature license usage, the table on the Usage by WebLM page remains blank.
IP address	The IP address of the master WebLM server and the local WebLM servers of the product.
Time of Query	The date and time when the system executes the last usage query for the WebLM server. If the status of the last usage query is `Failed`, the **Time of Query** column displays the date and time of the usage query that was last successful. **Note:** If the server does not receive a query request even once for feature license

Name	Description
	usage, the **Time of Query** column of a WebLM server remains blank.
Status	The success or failure of the last usage query that the system executes for each WebLM server. If the server does not receive a query request even once for feature license usage, the **Status** column of a WebLM server remains blank. The usage query can be a periodic usage query or a nonperiodic usage query.
Select Check box	Use to select the WebLM server for which you require to determine the usage query.

Button	Description
Check All	Selects all the WebLM servers.
Clear All	Clears the selections for all the WebLM servers.
Query Usage	Queries the WebLM servers of the product you select for their feature license usage report.

Related topics:

Querying usage of feature licenses for master and local WebLM servers on page 824

Allocations by Features field descriptions

Use this page to view the feature license allocation information for each counted type feature of the product.

Name	Description
Feature (License Keyword)	Specifies the name and license keyword of the counted features of the product.
Local WebLM Name	Specifies the name of the local WebLM servers of the product. By default, this column is blank. The system displays the names of the local WebLM servers only when you select the arrow head in the **Feature (License Keyword)** column. If a local WebLM server does not exist for the product, the **Local WebLM Name** column remains blank for all the licensed features.

Name	Description
IP address	Specifies the IP addresses of the local WebLM servers of the product. By default, this column is blank. The system displays the IP address of the local WebLM servers only when you select the arrow-head in the **Feature (License Keyword)** column. If a local WebLM server does not exist for the product, the **IP address** column remains blank for all the licensed features.
License Capacity	Specifies the total number of feature licenses purchased by the organization for the respective feature.
Currently Allocated	Specifies the total number of feature licenses of the respective feature that the system allocated to the local WebLM servers of the product. If a licensed feature is not allocated to any local WebLM server, the system displays `zero` in the **Currently Allocated** column for the licensed feature.
Available	Lists the number of floating licenses of the respective feature that is currently available with the master WebLM server.

Note:

To view the information about the number of feature licenses of a feature that the system allocates to each local WebLM server, click the arrow-head beside the name of the required feature. The system displays new rows below the feature row with the feature license allocation information for each local WebLM server to which the feature is allocated.

Related topics:

Viewing allocations by features on page 826

Allocations by Local WebLM field descriptions

Use this page to view the feature license allocation information by local WebLM.

Name	Description
Select Local WebLM	Specifies the local WebLM servers for which you can view the feature license allocation information.

Name	Description
Last Allocation	Specifies the date and time when feature licenses were last allocated to the local WebLM server you select.
Status	Specifies the success or failure status of the last license allocation process that the system executes for the local WebLM server you select. The allocation process can be a periodic allocation process or a nonperiodic allocation process. If the status of the last license allocation process is `Failed`, and if the status of a previous license allocation process for the server is `Success`, the system displays the date and time of the last license allocation process that was successful in the **Last Allocation** field.
Feature (License Keyword)	Specifies the name and license keyword of the counted features that the system allocates to the local WebLM server you select.
License Capacity	Specifies the total number of feature licenses the organization purchases for each feature.
Currently Allocated	Specifies the total number of feature licenses of each feature that the system allocates to the local WebLM server you select.
Available	Lists the number of licenses currently available on the master WebLM server for allocation to local WebLM servers.

Related topics:

Viewing allocations by the local WebLM server on page 826

Change Allocations field descriptions

Use this page to change current feature license allocation information for each local WebLM server of a product.

Name	Description
Feature (License Keyword)	The name and license keyword of the counted features that the system allocates to the local WebLM server you select.

Name	Description
Local WebLM Name	The name of the local WebLM server.
IP address	The IP addresses of the local WebLM servers of the product.
License Capacity	The total number of feature licenses that the organization purchases for each feature.
Currently Allocated	The total number of feature licenses of each feature that the system allocates to the local WebLM server you select.
Currently Used	The total number of feature licenses of each feature that the product uses.
Available	The number of floating licenses of each feature that is currently available with the local WebLM server.
New Allocation	The number of new licenses that the system allocates to a local WebLM server.

Button	Description
Submit Allocations	Allocates the number of feature licenses that you specify in the **New Allocation** field to the corresponding local WebLM servers.
Reset	Resets the values that you specify in the **New Allocation** field to the previously saved value.

Related topics:

Changing allocations of licensed features for a local WebLM server on page 825

Periodic Status field descriptions

Use the Periodic Status option to view the status of periodic operations such as the periodic allocation of the feature licenses to the local WebLM server and querying of the local WebLM server for usage report.

Periodic Allocation

Name	Description
Local WebLM Name	Specifies the name of the local WebLM server of a product.
IP Address	Specifies the IP addresses of all the local WebLM servers of the product.

Name	Description
Last Allocation	Displays the date and time when the system executed the last periodic license allocation process for each local WebLM server. If the status of the last periodic license allocation process is `Failed`, the **Last Allocation** column displays the date and time of the periodic license allocation process that was last successful.
Status	Displays the success or failure status of the last periodic license allocation process that the system executed for each local WebLM server.

Periodic Usage

Name	Description
WebLM Name	Displays the name of the master WebLM server and local WebLM servers of a product.
IP Address	Displays the IP addresses of the master and local WebLM servers of a product.
Last Usage Query	Displays the date and time when the system executed the last periodic usage query for each WebLM server. If the status of the last periodic usage query is `Failed`, the **Last Usage Query** column also displays the date and time of the periodic usage query that was last successful.
Status	Displays the success or failure status of the last periodic usage query that the system executed for each WebLM server. If the server is not queried even once for feature license usage, the **Status** column of a WebLM server remains blank.

Related topics:

Viewing the periodic status of the master and local WebLM servers on page 824

Overuse field descriptions

Use this page to specify the overuse value in percent for licensed features of a product.

Name	Description
Update percent overuse value	The overuse values in percent. For example, if there are 10 licenses available for a feature and you have set the overuse value to 50 percent then it indicates that you have 5 buffer licenses for the feature.

Button	Description
Submit	Sets the overuse value.
Reset	Set the values in the **Update percent overuse value** to the default value.

Related topics:

Specifying overuse limit for licensed features on page 824

Chapter 11: Data Replication Service

Data Replication Service

Data Replication Service (DRS) replicates data stored on the System Manager server to other element nodes or the slave nodes. DRS uses and extends SymmetricDS as the underlying mechanism for data replication.

SymmetricDS is an asynchronous data replication software that supports multiple subscribers and bi-directional synchronization. SymmetricDS uses Web and database technologies to replicate tables between relational databases in near real time. You can filter data as you record, extract, and load the data.

Databases provide unique transaction IDs to rows that are committed as a single transaction. SymmetricDS stores the transaction ID along with the data that changed, so that it can play back the transaction at the destination node exactly the way it happened. This means that the target database maintains the same integrity as the source.

DRS provides a mechanism wherein elements can specify their data requirements in an XML document. On the basis of the XML document, DRS creates database triggers on the specified application tables and captures the database events for delivery to other element nodes. The client nodes then fetch these database events.

Data replication happens in two distinct phases:

- Full-sync. This is the initial replication phase, wherein whatever data the replica node requests is replicated to the client node.
- Regular-sync. This is the phase after full-sync, wherein subsequent change events are replicated to the replica node.

DRS supports the following modes of replication:

- Replication in Repair mode. In the repair mode, DRS replicates all of the requested data from the master database to the database of the replica node. Repair should only be necessary if there is a post-install failure of DRS.
- Automatic synchronization mode. After the database of the replica node is loaded with the requested data, the subsequent synchronizations of the master database and the replica database occur automatically. DRS replicates only the data that has been updated since the last replication. Automatic synchronization is a scheduled activity and occurs after each fixed interval of time as set in the configuration files.

The data from the master database is sent to the replica node in batches. DRS creates replication batches whenever the data in the master database is added, modified, and deleted.

Using DRS, you can do the following :

- View replica nodes in a replica group.
- Perform a repair on the replica nodes that are not synchronized. This replicates the required data from System Manager.

Viewing replica groups

Procedure

On the System Manager Web Console, click **Services** > **Replication**.

Result

The system displays the Replica Groups page with the groups in a table.

Related topics:

Replica Groups field descriptions on page 855

Viewing replica nodes in a replica group

You can view the replica nodes in a group.

Procedure

1. On the System Manager Web Console, click **Services** > **Replication**.
2. On the Replica Groups page, select a replica group and click **View Replica Nodes**.

   Alternatively, you can click a replica group name displayed under the **Replica Group** column to view the replica nodes for that replica group.

   The Replica Nodes page displays the replica nodes for the select group.

Related topics:

Replica Nodes field descriptions on page 857

Repairing a replica node

You can replicate data for a replica node whose database is not synchronized with the System Manager database. Repair is necessary if there is a post-install failure of Data Replication Service.

Procedure

1. On the System Manager Web Console, click **Services** > **Replication**.
2. On the Replica Groups page, perform one of the following:
   - Select a replica group for which you want repair the replica nodes from the table displaying replica groups and click **View Replica Nodes**.
   - Click the name of the replica node under the **Replica Group** column.
3. On the Replica Nodes page, select a replica node and click **Repair**.

   The **Synchronization Status** column displays the data replication status for the repairing replica node.

Related topics:

Replica Nodes field descriptions on page 857

Repairing all replica nodes in a replica group

You can replicate data for all the replica nodes that are in a group. You can perform this operation if replica nodes in a group are not synchronized with the System Manager database.

Procedure

1. On the System Manager Web Console, click **Services** > **Replication**.
2. On the Replica Groups page, select a replica group for which you want repair the replica nodes from the table displaying replica groups.
3. Click **Repair**.

   The **Synchronization Status** column displays the data replication status for the replica group.

Viewing replication details for a replica node

You can view the batch related information such as total number of batches received, processed, and skipped for a replica node. The master database sends the requested data in batches to the replica node.

Procedure

1. On the System Manager Web Console, click **Services** > **Replication**.
2. On the Replica Groups page, select a replica group and click **View Replica Nodes**.
   The Replica Nodes page displays the replica nodes for the selected replica group in a table.
3. Select a replica node and click **View Details**.
   The Data Replication page displays the replication details for the selected replica node.

Related topics:

Replication Node Details field descriptions on page 859

Removing a replica node

Procedure

1. On the System Manager Web Console, click **Services** > **Replication**.
2. On the Replica Groups page, select a replica group in which you want to remove a node and click **View Replica Nodes**.
3. On the Replica Node page, click **Remove**.

Removing a replica node from queue

Procedure

1. On the System Manager Web Console, click **Services** > **Replication**.

2. On the Replica Groups page, select the replica group for which you want to remove the node from queue and click **View Replica Nodes**.
3. On the Replica Node page, click **Remove from Queue**.

Validating replica groups

About this task

You can use this validation tool to run certain basic configuration checks on the replica groups and the individual nodes.

Procedure

1. On the System Manager Web Console, click **Services** > **Replication**.
2. On the Replica Groups page, select the replica group you want to validate.
3. Click **Validate**.
   After the validation is complete, the status in the **Job Status** column in the **Diagnostic History** tab displays **Completed**.

Related topics:

DRS validation results on page 852
Validation Result field descriptions on page 861
Validation Result Details field descriptions on page 861

Validating System Manager

About this task

You can use the validation tool to check the basic System Manager configuration while deploying System Manager. You can use the validation tool even before you run other sanity checks.

Procedure

1. On the System Manager Web Console, click **Services** > **Replication**.
2. On the Replica Groups page click the **Diagnostic History** tab.
3. Click **Validate SMGR**.

The validation tool runs the validations on the current System Manager system. After the validation is complete, the **Job Status** column displays the **Completed** status.

Related topics:

DRS validation results on page 852
Validate SMGR field descriptions on page 854
Validation Result field descriptions on page 861
Validation Result Details field descriptions on page 861

Viewing validation results

Procedure

1. On the System Manager Web Console, click **Services** > **Replication**.
2. On the Replica Groups page click the **Diagnostic History** tab.
3. Select the host for which you want to view the validation result.
4. Click **View Result**.
   The system displays the Validation Result page with the **General** section and the **Validation Result** section.
5. To view the validation result details, click the **Validation Result** for each test in the **Validation Result** table.
   The system displays the Validation Result Details page with the **General** and **Result** sections.

Related topics:

Validation Result field descriptions on page 861
Validation Result Details field descriptions on page 861

DRS validation results

You can view the DRS validation test results in the View Result Details page. The results help you to locate any errors during System Manager deployment or during Session Manager installation or upgrade. The following tables provide the tests that you can run through the DRS tool.

Table 9: Common tests for System Manager, Session Manager, and Presence Services

Test	Purpose
check_basic_configurations	Verifies the basic configurations. You can ensure whether an entry is available for localhost in `/etc/hosts`.

Table 10: Tests for System Manager

Test	Purpose
check_master_hostname_alias	Verifies whether FQDN is configured properly in `/etc/hosts`.
check_master_fqdn_ping	Verifies whether the System Manager FQDN from `/etc/hosts` responds to ping.
check_avmgmt_db_exist	Verifies whether the avmgmt database exists.
check_master_node_id_matches_fqdn	Verifies whether the FQDN from the host matches the DRS master node ID.
check_replica_nodes_ping	Checks whether all the replicas respond to ping.
check_duplicate_node_ids	Verifies that there are no duplicate nodes in DRS configuration.
check_missing_trigger_methods	Verifies whether DRS triggers are configured properly.
check_drs_sds_data_matches	Verifies whether the SymmetricDS configuration matches the DRS management configuration.
check_nrp_bwc_triggers_and_data	Verifies whether all the records of *ingressadaptation with phone_context*are null, and exist in *ingressadaptation_6_0*.
check_errors_in_symmetric_log_file	Checks for error messages in the `/var/log/Avaya/mgmt/drs/symmetric.log` symmetric log file.
check_required_patches_installed	Verifies whether you have installed the required patches in System Manager.
check_symmetric_properties_file	Verifies whether the properties are set correctly in `/opt/Avaya/JBoss/4.2.3/jboss-4.2.3.GA/jboss-as/server/avmgmt/deploy/symmetricds.war/WEB-INF/classes/symmetric.properties`.

Table 11: Tests for Session Manager

Test	Purpose
check_replica_hostname_alias	Verifies whether FQDN is configured properly in `/etc/hosts`.
check_replica_fqdn_ping	Verifies whether the Session Manager FQDN from `/etc/hosts` responds to ping.
check_presence_db_exist	Checks whether the Presence database exists.
check_asm_db_exist	Verifies whether the asm database exists.
check_master_node_ping	Checks whether System Manager responds to ping.
check_for_error_batches	Checks for error batches.
check_initial_load_enabled_state	Checks whether the initial load is in the enabled state.
check_errors_in_symmetric_log_file	Checks for error messages in the `/var/log/Avaya/mgmt/drs/symmetric.log` symmetric log file.
check_certificate	Verifies that there are no certificate problems when connecting to System Manager.
check_smgr_date_smaller_than_replica_date	Verifies whether the date in System Manager is less than or equal to the replica date.
check_replica_version_compatible_with_smgr_version	Verifies whether the version of replica is compatible with System Manager.
check_replicated_tables_exist_on_replica	Verifies whether all the tables that you need to replicate to this replica node exist in the database.

Validate SMGR field descriptions

Name	Description
Replica Node Host Name	Specifies the host name of System Manager. If you are using this page to administer Session Manager, the system displays the fully qualified domain name. For example, sv-st10-lspj-bsm.dsvdata.com.

Name	Description
Replica Group	Specifies the name of the replica group.
Job Status	Status of the validation. Possible values include: **Running**, **Failed** , and **Completed**.
Initiated by	Specifies the username of the user who initiated the System Manager validation.
Validation Start Time	Specifies the time when you started the System Manager validation job.

Button	Description
Validate SMGR	Validates the System Manager you selected from the list.
View Result	Displays the validation results of the System Manager you select from the table.

Replica Groups field descriptions

The replica groups are logical grouping of the replica nodes. You can use the replica groups field descriptions page to:

- View all the replica groups in the enterprise.
- Replicate data requested by the replica node from the master database to the database of the replica nodes.
- View the replication status of the replica groups.
- Check the basic System Manager configuration while you deploy System Manager.
- View the results of the basic checks.

Replica Groups tab

The page displays the following fields when you select `All` from the **Replica Group** field.

Name	Description
Select check box	Provides an option to select a replica group.
Replica Group	Specifies the name of the replica group. Each replica group in the list is a hyperlink. When you click a group, the Replica Nodes page opens and displays the replica nodes for that group.

Name	Description
Synchronization Status	For each replica group, displays the combined synchronization status of all replica nodes under the group

Button	Description
View Replica Nodes	Opens the Replica Nodes page. Use this page to view replica nodes for a group you select.
Repair	Initiates full-sync for the selected groups and effectively for all the replica nodes that belong to the selected groups.
Validate	Validates the replica groups for basic configuration.

Diagnostic History tab

The page displays the following fields when you select `All` from the **Record Node Host Name** field.

Name	Description
Select check box	Provides an option to select a replica group.
Replica Node Host Name	Specifies the full hostname of the replica node. If you are using this page to administer Session Manager, the system displays the fully qualified domain name. For example, ab-ct10-defg-bsm.mydata.com.
Replica Group	Specifies the name of the replica group.
Job Status	Status of the validation. The possible values include: **Running**, **Failed**, and **Completed**.
Initiated By	Specifies the username of the user who initiated the System Manager validation.
Validation Start Time	Specifies the time when you started the System Manager validation job.

Button	Description
Validate SMGR	Validates the node you selected from the list.
View Result	Displays the validation results of the node you selected from the list.

Replica Nodes field descriptions

You can use this page to:

- View the replica nodes in a selected replica group when you request data replication from the master database of System Manager.
- View the replication status of the replica nodes in a group.

Name	Description
Select check box	Provides the option to select a replica node.
Replica Node Host Name	Specifies the full hostname of the replica node. If you are using this page to administer Session Manager, the system displays the fully qualified domain name. For example, ab-ct10-defg-bsm.mydata.com.
Product	Specifies the name of the product.
Synchronization Status	Specifies the synchronization status of the replica node. When a node is installed, it goes from a **Ready for Repair** state to the **Queued for Repair** to **Repairing**, and finally to **Synchronized**. During this phase, the replica node receives a full-sync, wherein configured data is replicated to the replica node. Once the replica node is prepared with a full-sync, thereafter the node receives the subsequent changes in the form of regular-sync. The data replication for a replica node begins with a full-sync and continues with regular-sync for the node. A replica node can be in any one of the following states during its lifecycle: • **Ready for Repair**: The database of the replica node is not synchronized with the master database. • **Queued for Repair**: The request for initiating full-sync for the node is in queue with other full-sync requests. The color code of the status is yellow.

Name	Description
	• **Repairing**: The full-sync for the replica node is in progress. The color code of the status is yellow. • **Synchronized**: The system successfully replicated the data that the replica node requested from the master database to the database of the replica node. The color code of the status is green. **Note:** If you encounter the following, contact the administrator who can manually intervene to resolve the problem: • `Not Reachable`: System Manager is unable to connect to the replica node. This indicates that the replica node is switched off for maintenance, a network connectivity failure, or any other issue that affects general connectivity between System Manager and the replica node. • `Synchronization Failure`: Data replication is broken between System Manager and the replica node. This status generally indicates a catastrophic failure. The system displays the following status during automatic replication of data from the master to the replica node: • **Synchronizing**. The data replication is in progress for the replica node. The color code of the status is yellow. • **Synchronized**. The system successfully replicated the data that the replica node requested from the master database to the database of the replica node. The color code of the status is green.
Last Synchronization Time	Specifies the last time when the system performed the data synchronization or replication for the replica node.

Button	Description
View Details	Opens the Data Replication page. Use this page to view the synchronization details for a replica node.
Repair	Replicates or resynchronizes data from the master node to a selected replica node.
Validate	Validates a replica node for basic configuration.
Remove	Removes the nodes you select from the replica group.
Remove From Queue	Removes the replica node you select from the queue.
Show All Replica Groups	Takes you back to the Replica Groups page.

Replication Node Details field descriptions

You can use this page to view the following details:

- The batch related information such as total number of batches received, processed, and skipped for a replica node.
- The last time when the replication server performed the synchronization or replication.
- Synchronization or replication error details.

General

Name	Description
Replica Node Group	Specifies the name of the group that the replica node belongs to. A node-group is a logical grouping of similar nodes.
Replica Node Host Name	Specifies the full hostname of the replica node. If you are using this page to administer Session Manager, the system displays the fully qualified domain name. For example, ab-ct10-defg-bsm.mydata.com.
Last Synchronization Time	Specifies the last time and date when the system performed the data synchronization or replication for the replica node.

Name	Description
Last Down Time	Specifies the last time and date when the replica node could not be reached. System Manager periodically checks whether a replica node is reachable.
Last Repair Start Time	Specifies the last time and date when a full-sync was started for the node.
Last Repair End Time	Specifies the last time and date when a full-sync was completed for the node.
Synchronization Status	Specifies the synchronization status of the replica node.

Synchronization Status

Name	Description
Pending Batches	Specifies the batches which are yet to be replicated to the replica node. During the data replication process, System Manager records the changes for a particular replica node in the form of events. When a replica node requests System Manager for change events, the change events are made into batches. These batches are then replicated to the replica node.
Pending Unbatched Events	Specifies the change events that are yet to be formed into batches. The recorded change events are formed into batches and only a predefined number of batches are replicated to a replica node in a request. The remaining events wait for the subsequent request from the replica and are called unbatched events pending batching and subsequent replication.

Last Error Details

Name	Description
Cause of Error	Describes why the system failed to replicate or synchronize data.
Time of Error	Specifies the time when the error occurred.

Validation Result field descriptions

General section

Name	Description
Replica Group	Specifies the name of the replica group.
Replica Node Host Name	The host name of the System Manager.
Job Id	Job Id of the validation job.
Initiated By	Specifies the username of the user who initiated the validation.
Validation Start Time	Specifies the time in which you start the validation job.
Validation End Time	Specifies the time the validation job was completed.

Validation Result section

Name	Description
Validation Name	Name of the validation test.
Validation Result	Specifies whether the validation is successful or has an error.
Description	Description of the validation test.

Button	Description
Done	Completes your action and takes you to the back to the Replica Groups page.

Validation Result Details field descriptions

General section

Name	Description
Replica Group	Specifies the name of the replica group.
Replica Node Host Name	The host name of the System Manager.

Name	Description
Validation Name	Name of the validation test.

Result section

Name	Description
Result	Specifies whether the validation successful or has an error.
Description	Description of the validation test.
Output	Displays the output of the validation test.

Button	Description
Done	Takes you back to the Validation Result page.

Related topics:

Validate SMGR field descriptions on page 854

Validate SMGR field descriptions

Name	Description
Replica Node Host Name	Specifies the host name of System Manager. If you are using this page to administer Session Manager, the system displays the fully qualified domain name. For example, sv-st10-lspj-bsm.dsvdata.com.
Replica Group	Specifies the name of the replica group.
Job Status	Status of the validation. Possible values include: **Running**, **Failed** , and **Completed**.
Initiated by	Specifies the username of the user who initiated the System Manager validation.
Validation Start Time	Specifies the time when you started the System Manager validation job.

Button	Description
Validate SMGR	Validates the System Manager you selected from the list.

Button	Description
View Result	Displays the validation results of the System Manager you select from the table.

Chapter 12: Managing scheduled jobs

Scheduler

The Scheduler service is designed to provide a generic job scheduling service for System Manager and the adopting products. The Scheduler service provides an interface to execute a task on demand or on a periodic basis. You can schedule a job to generate an output now, or set the frequency of task execution to run on a periodic basis. You can also modify the frequency for a periodic job schedule any time.

The scheduled job or the task definition is in the form of a job type XML. The Scheduler service parses the xml and persists the information in the System Manager database. After you define a task or a job, System Manager creates instances of the task, monitors the execution of the task, and updates the status of the task.

Scheduled tasks are of three types:

- System scheduled: System Scheduled jobs are executed on a periodic basis for a stable functioning of the system. The system adds these jobs at start-up time and supports all frequencies other than “One Time”. As an administrator you cannot add or delete system-scheduled jobs. You can only disable or enable these jobs in order to suspend temporary operations. Scheduled jobs run asynchronously in the background.
- Admin scheduled job: The job that the administrator schedules for administering the application. To populate the job parameters, call a service. The job parameters are in read-only format.
- On-demand job: Administrators schedule these jobs for non-routine, one time tasks. Administrators schedule On-demand jobs to run only once; the job metadata is stored in the database.

You can browse the history of completed jobs. Using the Disable functionality, you can cancel all the executions scheduled for a task. The following are some of the operations that you can perform using the scheduler service:

- View the pending and completed scheduled tasks.
- Modify a task scheduled by an administrator or an on-demand job.
- Delete a scheduled task.
- Schedule an on-demand job.
- Stop a running task.

- Enable or disable a task.
- Search a scheduled task.

Accessing scheduler

Procedure

On the System Manager Web Console, click **Services** > **Scheduler**.

Viewing pending jobs

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. In the left navigation pane, click **Pending Jobs**.

Related topics:

Pending Jobs field descriptions on page 873

Viewing completed jobs

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. Click **Completed Jobs** in the left navigation pane.
   The Completed Jobs page displays completed jobs.

Related topics:

Completed Jobs field descriptions on page 875

Viewing details of a pending job

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. In the left navigation pane, click **Pending Jobs**.
3. On the Pending Jobs page, select a pending job and click **View**.
   The Job Scheduling-View Job page displays the details of the selected job.

Viewing details of a completed job

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. In the left navigation pane, click **Completed Jobs**.
3. On the Completed Jobs page, select a completed job and click **View**.
   The Job Scheduling-View Job page displays the details of the selected job.

Viewing details of a pending job

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. In the left navigation pane, click **Pending Jobs**.
3. On the Pending Jobs page, select a pending job and click **View**.
   The Job Scheduling-View Job page displays the details of the selected job.

Viewing logs for a job

About this task

Use this functionality to view logs for a pending and completed job.

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To view logs for a pending job, perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job and click **More Actions** > **View Log**.
   - To view logs for a competed job, perform the following steps:
     i. Click **Completed Jobs** in the left navigation pane.
     ii. On the Completed Jobs page, select a completed job and click **More Actions** > **View Log**.

   The log viewer displays the log details for the selected job.

Viewing completed jobs

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. Click **Completed Jobs** in the left navigation pane.
   The Completed Jobs page displays completed jobs.

Related topics:

Completed Jobs field descriptions on page 875

Filtering jobs

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. Perform one of the following:
   - To filter pending jobs:
     i. Click **Pending Jobs** in the left navigation pane
     ii. On the Pending Jobs page, click **Filter: Enable**.
   - To filter completed jobs:
     i. Click **Completed Jobs** in the left navigation pane
     ii. On the Completed Jobs page, click **Filter: Enable**.

   The system displays the **Filter: Enable** option at the upper-right corner of the page.
3. Select the type of the job from the field under the **Job Type** column.
4. Enter the name of job in the field under the **Job Name** field.
5. Select the status of the job from the field under the **Job Status** field.
6. Select the state of the job from the field under the **State** field.
7. Select the frequency of execution of the job from the field under the **Frequency** field.
8. Enter the scheduler of the job in the field under the **Scheduled By** column.

   Note:

   The system displays this field only for the completed jobs.
9. Click **Apply**.
   The system displays jobs that match the filter criteria.

Editing a job

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.

2. Perform one of the following steps:
   - To edit a pending job, perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job and click **Edit** or click **View** > **Edit**.
   - To edit a competed job, perform the following steps:
     i. Click **Completed Jobs** in the left navigation pane.
     ii. On the Completed Jobs page, select a completed job and click **Edit** or click **View** > **Edit**.
3. On the Job Scheduling-Edit Job page, modify the appropriate information and click **Commit** to save the changes.

   You can modify information in the following fields: **Job Name**, **Job State** in the Job Details sections, and **Task Time**, **Recurrence**, **Range** in the Job Frequency section.

Deleting a job

Before you begin

You have logged in as an administrator to delete an administrator scheduled job.

About this task

Use this functionality to delete an obsolete job. You can delete an on-demand and an administrator scheduled job.

Note:

You can remove only **Schedule On Demand** type of jobs.

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To remove a pending job, perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job.

     If the job that you want to delete is currently running then you must stop the job. To stop the job, click **More Actions** > **Stop**.

Note:

If the job that you want to delete is in the enabled state, disable the job. See Disabling a job on page 871on how to disable a job.

iii. Click **Delete**.

- To remove a competed job, perform the following steps:

i. Click **Completed Jobs** in the left navigation pane.

ii. On the Completed Jobs page, select a completed job.

Note:

If the job that you want to delete is in the enabled state, disable the job.

iii. Click **Delete**.

3. On the Delete Confirmation page, click **OK**.
   System Manager deletes the job you select from the database.

Disabling a job

About this task

Use this functionality to make a job inactive.

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To disable a pending job, perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job and click **More Actions** > **Disable**.
   - To disable a competed job, perform the following steps:
     i. Click **Completed Jobs** in the left navigation pane.
     ii. On the Completed Jobs page, select a completed job and click **More Actions** > **Disable**.
3. On the Disable Confirmation page, click **Continue**.

The **State** of the job you selected changes to **Disabled**.

Enabling a job

About this task

Use this functionality to make a job active.

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To enable a pending job, perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job and click **More Actions** > **Enable**.
   - To enable a competed job, perform the following steps:
     i. Click **Completed Jobs** in the left navigation pane.
     ii. On the Completed Jobs page, select a completed job and click **More Actions** > **Enable**.

   The **State** of the selected job is changed to **Enabled**.

Result

Stopping a job

Procedure

1. On the System Manager Web Console, click **Services** > **Scheduler**.
2. In the left navigation pane, click **Pending Jobs**.
3. On the Pending Jobs page, select a pending job in the running state and click **More Actions** > **Stop**.
4. Click **Continue** on the Stop Confirmation page.
   Scheduler stops the selected job.

Pending Jobs field descriptions

Use this page to view, edit, and delete the scheduled jobs that are pending for execution.

Name	Description
Job Type	Specifies the type of job represented by an icon that corresponds to its type. The application uses different icons to represent the job types. The types of job are: 1. System scheduled job. The job scheduled for the normal operation of the application. A system administrator can reschedule and stop a system schedule job, but cannot delete the job. 2. Admin scheduled job. The job that an administrator schedules for administering the application. 3. On-demand job. The periodic jobs that an administrator may schedule to perform non-routine tasks.
Job Name	Specifies the name of the scheduled job.
Job Status	Specifies the current status of the pending job. The types of status are: 1. Pending Execution 2. Running
State	Specifies the state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.
Frequency	Specifies the time interval between two consecutive executions of the job.
Scheduled By	Specifies the scheduler of the job.

Button	Description
View	Opens the Job Scheduling-View Job page that displays the details of the selected pending job.

Button	Description
Edit	Opens the Job Scheduling-Edit Job page that you can use to modify the information of a selected pending job.
Delete	Opens the Delete Confirmation page that prompts you to confirm the deletion of the selected jobs.
More Actions > **View Log**	Opens the Logging page that displays the logs for the selected pending jobs.
More Actions > **Stop**	Stops the selected job which is currently in the running state.
More Actions > **Enable**	Changes the state of the selected pending job from inactive to active.
More Actions > **Disable**	Opens the Disable Confirmation page that prompts you to confirm the disabling of the selected pending job.
More Actions > **Schedule On Demand Job**	Opens the Job Scheduling-On Demand Job page that you can use to schedule the selected pending job of type On Demand.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a pending job.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. **Filter: Enable** is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Apply	Filters pending jobs based on the filter criteria.
Select: All	Selects all the pending jobs in the table displayed in the **Job List** section.
Select: None	Clears the selection for the pending jobs that you have selected.
Refresh	Refreshes the pending job information.

Criteria section

To view this section, click **Advanced Search**. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Criteria	Displays the following three fields:

Name	Description
	• Drop-down 1– The list of criteria that you can use to search the pending jobs. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the pending jobs based on the specified search conditions and displays the search results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

Related topics:

Viewing pending jobs on page 866

Completed Jobs field descriptions

Use this page to view and edit completed jobs. In addition, you can also perform the following operations:

- Disable or enable a job.
- View a log.
- Schedule and delete an on-demand job.

Name	Description
Job Type	Specifies the type of job represented by an icon that corresponds to its type. The application uses different icons to represent the job types. The types of job are: 1. System scheduled job. The job scheduled for the normal operation of the application. A system administrator

Name	Description
	can reschedule and stop a system schedule job, but cannot delete the job. 2. Admin scheduled job. The job that an administrator schedules for administering the application. 3. On-demand job. The periodic jobs that an administrator may schedule to perform non-routine tasks.
Job Name	Specifies the name of the scheduled job.
Job Status	Specifies the current status of the pending job. The types of status are: 1. Status Unknown 2. Interrupted 3. Failed 4. Successful 5. Not Authorized
Last Run	Specifies the date and time when the job was last run.
State	Specifies the state of a job, whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.
Frequency	Specifies the time interval between two consecutive executions of the job.
Scheduled By	Specifies the scheduler of the job.

Button	Description
View	Opens the Job Scheduling-View Job page that displays the details and of the selected completed job.
Edit	Opens the Job Scheduling-Edit Job page that you can use to modify the information of a selected completed job.
Delete	Opens the Delete Confirmation page that prompts you to confirm the deletion of the selected Jobs.

Button	Description
More Actions > **View Log**	Opens the Logging page that displays the logs for the selected completed jobs.
More Actions > **Enable**	Changes the state of the selected completed job from inactive to active.
More Actions > **Disable**	Opens the Disable Confirmation page that prompts you to confirm the disabling of the selected completed job.
More Actions > **Schedule On Demand Job**	Opens the Job Scheduling-On Demand Job page that you can use to schedule a On Demand job.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a completed job.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters pending jobs based on the filter criteria.
Select: All	Selects all the completed jobs in the table displayed in the Job List section.
Select: None	Clears the selection for the completed jobs that you have selected.
Refresh	Refreshes the completed job information.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Criteria	Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search the completed jobs. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion

Name	Description
	that you have selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the completed jobs based on the specified search conditions and displays the search results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

Related topics:

Viewing completed jobs on page 866

Job Scheduling-View Job field descriptions

Use this page to view the details and frequency of a job.

Job Details

Name	Description
Job Name	Specifies the name of the job.
Job Type	Specifies the type of job represented by an icon that corresponds to its type. The application uses different icons to represent the job types. The types of job are: 1. System scheduled job. The job scheduled for the normal operation of the application. A system administrator

Name	Description
	can reschedule and stop a system schedule job, but cannot delete the job. 2. Admin scheduled job. The job that an administrator schedules for administering the application. 3. On-demand job. The periodic jobs that an administrator may schedule to perform non-routine tasks.
Job Status	Specifies the current status of the job. The types of status are: 1. Running 2. Pending 3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized
Job State	Specifies the state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.

Job Frequency

Name	Description
Task Time	Specifies the date and time of running the job.
Recurrence	Specifies the settings that define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field also displays the frequency of recurrence.
Range	Specifies the number of recurrences or a date after which the job stops to recur.

Button	Description
View Log	Opens the Logging page that you can use to view the logs for the selected job.

Button	Description
Edit	Opens the Job Scheduling-Edit Job page that you can use to edit the pending job information.
Cancel	Closes the Job Scheduling-View Job page and returns to the Pending or Completed Jobs page.

Job Scheduling-Edit Job field descriptions

Use this page to modify job details and frequency related information of a selected job.

Job Details

Name	Description
Job Name	Specifies the name of the job.
Job Type	Specifies the type of job represented by an icon that corresponds to its type. The application uses different icons to represent the job types. The types of job are: 1. System scheduled job. The job scheduled for the normal operation of the application. A system administrator can reschedule and stop a system schedule job, but cannot delete the job. 2. Admin scheduled job. The job that an administrator schedules for administering the application. 3. On-demand job. The periodic jobs that an administrator may schedule to perform non-routine tasks. **Note:** You can only view the information in this field.
Job Status	Specifies the current status of the job. The types of status are: 1. Running 2. Pending 3. Status Unknown

Name	Description
	4. Interrupted 5. Failed 6. Successful 7. Not Authorized **Note:** You can only view the information in this field.
Job State	Specifies the state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.
Scheduled By	Specifies the scheduler of the job. **Note:** You can only view the information in this field.

Job Frequency

Name	Description
Task Time	Specifies the date and time of running the job. Use the calendar icon to select a date. The time is in the HH:MM:SS format followed by PM and AM.
Recurrence	Specifies the settings that define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field displays the frequency of recurrence.
Range	Specifies the number of recurrences or the date after which the job stops to recur.

Button	Description
Commit	Saves the changes to the database.
Cancel	Closes the Job Scheduling-View Job page and returns to the Pending or completed Jobs page.

Job Scheduling-On Demand Job field descriptions

Use this page to schedule an on-demand job.

Job Details

Name	Description
Job Name	Specifies the name of the job.

Job Frequency

Name	Description
Task Time	Specifies the date and time of running the job.
Recurrence	Specifies the settings that define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field also display the time interval of recurrence. The options are: • Execute task one time only. • Task are repeated every day.
Range	Specifies the settings that define the number of recurrences or date after which the job stops recurring. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules an On-Demand job.
Cancel	Cancels the schedule an On Demand job operation and takes you back to the Pending or completed Jobs page.

Disable Confirmation field descriptions

Use this page to disable selected jobs.

Name	Description
Job Type	Specifies the type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. The types of job are: 1. System scheduled job. The job scheduled for the normal operation of the application. A system administrator can reschedule and stop a system schedule job, but cannot delete the job. 2. Admin scheduled job. The job that an administrator schedules for administering the application. 3. On-demand job. The periodic jobs that an administrator may schedule to perform non-routine tasks.
Job Name	Specifies the name of the scheduled job.
Job Status	Specifies the current status of the pending job. The types of status are: 1. Running 2. Pending 3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized
State	Specifies the state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.
Last Run	Specifies the date and time when the job was last run successfully.

Name	Description
	Note: The last run is applicable only for completed jobs.
Frequency	Specifies the time interval between two consecutive executions of the job.
Scheduled By	Specifies the scheduler of the job.

Button	Description
Continue	Disables the job and cancels the next executions that are scheduled for the job.
Cancel	Cancels the operation of disabling a job and takes you back to the Pending or completed Jobs page.

Stop Confirmation field descriptions

Use this page to stop a running job.

Name	Description
Job Type	Specifies the type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. The types of job are: 1. System scheduled job. The job scheduled for the normal operation of the application. A system administrator can reschedule and stop a system schedule job, but cannot delete the job. 2. Admin scheduled job. The job that an administrator schedules for administering the application. 3. On-demand job. The periodic jobs that an administrator may schedule to perform non-routine tasks.
Job Name	Specifies the name of the scheduled job.

Name	Description
Job Status	Specifies the current status of the pending job. The jobs on this page have status Running.
State	Specifies the state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job. All the jobs on this page are in the **Enabled** state.
Last Run	Specifies the date and time when the job was last run successfully. **Note:** The last run is applicable only for completed jobs.
Frequency	Specifies the time interval between two consecutive executions of the job.
Scheduled By	Specifies the scheduler of the job.

Button	Description
Continue	Stops the job.
Cancel	Cancels the operation of stopping a job and takes you back to the Pending Jobs page.

Delete Confirmation field descriptions

Name	Description
Job Type	Specifies the type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. The types of job are: 1. System scheduled job. The job scheduled for the normal operation of the application. A system administrator

Name	Description
	can reschedule and stop a system schedule job, but cannot delete the job. 2. Admin scheduled job. The job that an administrator schedules for administering the application. 3. On-demand job. The periodic jobs that an administrator may schedule to perform non-routine tasks.
Job Name	Specifies the name of the scheduled job.
Job Status	Specifies the current status of the job.
State	Specifies the state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job. The jobs on this page are in the **Disabled** state.
Last Run	Specifies the date and time when the job was last run. **Note:** The last run is applicable only for completed jobs.
Frequency	Specifies the time interval between two consecutive executions of the job.
Scheduled By	Specifies the scheduler of the job.

Button	Description
Continue	Deletes the selected job.
Cancel	Cancels the operation of deleting a job and takes you back to the Pending or completed Jobs page.

Chapter 13: Templates

Template management

A template is a file that contains stored settings. You can use templates to streamline the process of performing various routine activities. Templates save the data that you enter so that you can perform similar activities later without re-entering the same data. With System Manager, you can create, store, and use templates to simplify tasks like adding, editing, and viewing endpoints or subscribers. In System Manager, there are several default templates and you can create your own templates as well.

Templates exist in two categories, default templates and user-defined templates. The default templates exist on the system and you cannot edit or remove them. You can, however, modify or remove user-defined templates any time.

Template versioning

Template versioning

You can version endpoint templates with CM 5.0, CM 5.1, CM 5.2, CM 6.0, and CM 6.2. You can associate a template with a specific version of an adopting product through template versioning. You can use the **Template Version** field under endpoint templates to accommodate endpoint template versioning.

You can also use template versioning for subscriber templates using the following versions: Aura Messaging 6.1, Aura Messaging 6.0, MM 5.0, MM 5.1, MM 5.2, CMM 5.2, CMM 6.0 and CMM 6.2.

Filtering templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. Click either **Endpoint** or **Messaging** for endpoint templates and messaging templates respectively.

3. Select the Communication Manager or supported messaging version, whichever applicable.
4. Click **Show List**.
5. Click **Filter: Enable** in the Template List.
6. Filter the endpoint or subscriber templates according to one or multiple columns.
7. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

Note:

The table displays only those endpoint or subscriber templates that match the filter criteria.

Upgrading a template

Use this feature to upgrade an existing Communication Manager template to a later Communication Manager release. You can upgrade only custom templates. This feature supports upgrading a Communication Manager agent or endpoint template from an earlier Communication Manager release to a subsequent Communication Manager release. You can also upgrade templates across multiple releases.

This feature does not support downgrading of template versions.

When you perform the upgrade operation, note that:

- System migrates the existing template settings to the new template version.
- System sets the new parameters in the new template version to default values.
- System deletes the deleted parameters in the new template version as compared to the older template version.
- System makes the new keywords available for editing within the new template, but the upgraded template retains the previous keyword setting, if available. If the previous keyword is not available, then the default is used in the upgraded template.

After you commit a template upgrade task, the system upgrades the template and enlists the newly upgraded template on the Template List.

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. Click **CM Endpoint** in the left navigation pane.

3. Select the Communication Manager system whose custom template you want to upgrade from the list under **Supported Feature Server Versions**.

   You can upgrade only custom templates.

4. Click **Show List**.
5. Select the custom template that you want to upgrade from **Template List**.
6. Click **Upgrade**.
7. On the Upgrade Endpoint Template page, select the Communication Manager version for template upgrade from the list in **Supported CM Version**.
8. In the **Template Name** text box, enter the new name for the template.
9. Click **Upgrade**. The system updates **Template List** with the newly upgrade template.

Adding CM Agent template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Agent**.
3. Click **New**.
4. Enter a name in the **Template Name** field.
5. Complete the mandatory fields under the **General Options** and **Agents Skills** tabs.
6. Click **Commit**.

Related topics:

Add Agent Template field descriptions on page 900

Editing CM Agent template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Agent**.

3. Select the template you want to edit from the Templates List.

   Note:

   You cannot edit default templates.

4. Click **Edit** or click **View** > **Edit**.
5. Complete the **Edit Agent Template** page.
6. Click **Commit** to save the changes.

Related topics:

Add Agent Template field descriptions on page 900

Viewing CM Agent template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Agent**.
3. Select the template you want to view from the Templates List.
4. Click **View**.

   You can view the **General Options** and **Agent Skills** sections on the View Agent Template page.

Related topics:

Add Agent Template field descriptions on page 900

Deleting CM Agent template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Agent**.
3. Select the template you want to delete from the Templates List.

Note:

You cannot delete default templates.

4. Click **Delete**.

Duplicating CM Agent template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Agent**.
3. Select the template you want to copy from the Templates List.
4. Click **Duplicate**.
5. Complete the **Duplicate Agent Template** page.
6. Click **Commit**.

Related topics:

Add Agent Template field descriptions on page 900

Adding CM Endpoint templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Endpoint**.
3. Click **New**.
4. Click **Set type**.
5. Enter a name in the **Template Name** field.
6. Complete the mandatory fields under the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.
7. Click **Commit**.

Related topics:

Endpoint / Template field descriptions on page 550

Editing CM Endpoint templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Endpoint**.
3. Select the template you want to edit from the template list.
4. Click **Edit** or click **View** > **Edit**.
5. Complete the **Edit Endpoint Template** page.
6. Click **Commit** to save the changes.

Related topics:

Endpoint / Template field descriptions on page 550

Viewing CM Endpoint templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Endpoint**.
3. Select the template you want to view.
4. Click **View**.
   You can view the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Call Dialing**, **Enhanced Call Fwd**, and **Button Assignment** sections on the View Endpoint Template page.

Related topics:

Endpoint / Template field descriptions on page 550

Deleting CM Endpoint templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Endpoint**.
3. Select the endpoint templates you want to delete from the endpoint template list.
4. Click **Delete**.

Note:

You cannot delete any of the default templates.

Duplicating CM Endpoint templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Endpoint**.
3. Select the template you want to copy from the endpoint template list.
4. Click **Duplicate**.
5. Enter the name of the new template in the **New Template Name** field.
6. Choose the appropriate set type from the **Set Type** field.
7. Complete the **Duplicate Endpoint Template** page and click **Commit**.

Related topics:

Endpoint / Template field descriptions on page 550

Adding subscriber templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. Select a messaging version from the list of supported messaging versions.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions** and **Miscellaneous** sections in the Add Subscriber Template page.
7. Click **Commit**.

   Subscriber templates have different versions based on the software version. The subscriber templates you create have to correspond to the Messaging, MM, or CMM software version. When you select a messaging template, the **Software Version** field in the Add Subscriber Template page displays the appropriate version information.

Related topics:

Subscriber Messaging Templates field descriptions on page 928
Subscriber CMM Templates field descriptions on page 931
Subscriber MM Templates field descriptions on page 934

Editing subscriber templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. From the supported messaging version list, select a messaging version.
4. Click **Show List**.
5. Select a subscriber template from the Subscriber Template list.
6. Click **Edit** or **View** > **Edit**.

7. Edit the required fields on the **Edit Subscriber Template** page.
8. Click **Commit** to save the changes.

Note:

You cannot edit any of the default subscriber templates.

Related topics:

Subscriber Messaging Templates field descriptions on page 928
Subscriber CMM Templates field descriptions on page 931
Subscriber MM Templates field descriptions on page 934

Viewing subscriber templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. From the supported messaging versions list, select one of the messaging versions.
4. Click **Show List**.
5. Select a subscriber template from the Subscriber Template list.
6. Click **View** to view the mailbox settings of this subscriber.

Note:

You cannot edit any of the fields in the View Subscriber Template page.

Related topics:

Subscriber Messaging Templates field descriptions on page 928
Subscriber CMM Templates field descriptions on page 931
Subscriber MM Templates field descriptions on page 934

Deleting subscriber templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. From the list of supported messaging versions, select a supported messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select the templates you want to delete.
6. Click **Delete**.

Note:

You cannot delete any default subscriber template.

Duplicating subscriber templates

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. From the list of supported messaging versions, select a messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select the subscriber template you want to copy.
6. Click **Duplicate**.
7. Complete the Duplicate Subscriber Template page and click **Commit**.

Related topics:

Subscriber Messaging Templates field descriptions on page 928
Subscriber CMM Templates field descriptions on page 931
Subscriber MM Templates field descriptions on page 934

Viewing associated subscribers

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. From the list of supported messaging versions, select a messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select a subscriber template for which you want to view the associated subscribers.
6. Click **More Actions** > **View Associated Subscribers**.
   You can view all the associated subscribers in the System Manager database for the template you have chosen in the Associated Subscribers page.

Templates List

You can view Templates List when you click **Template** under **Services** on the System Manager console.

You can apply filters and sort each of the columns in the Template List. When you click **Refresh**, you can view the updated information available after the last synchronization operation.

B5800 Endpoint Templates

Name	Description
Name	Name of the template.
System Type	Specifies the name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template.
Version	Specifies the change version of the template.
Set Type	Specifies the set type of the branch gateway endpoint template.

Name	Description
Last Modified Time	Specifies the time and date when the template was last modified.

Name	Description
Name	Name of the template.
Owner	Specifies the name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template.
Version	Specifies the change version of the template.
Default	Specifies whether the template is default or user-defined.
Last Modified	Specifies the time and date when the endpoint or messaging template was last modified.
Set type (for endpoint templates)	Specifies the set type of the endpoint template.
Type (for messaging templates)	Specifies whether the messaging type is Messaging, MM, or CMM.
Software Version	Specifies the software version of the element for the template.

B5800 System Configuration template

Name	Description
Name	Name of the template.
System Type	Specifies the name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template.
Version	Specifies the change version of the template.
Last Modified Time	Specifies the time and date when the template was last modified.

CM Agent template

Name	Description
Name	Name of the template.
Owner	Specifies the name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template.
Version	Specifies the change version of the template.
Default	Specifies whether the template is default or user-defined.
Software Version	Specifies the software version of the element for the template.
Last Modified	Specifies the time and date when the template was last modified.

CM Endpoint template

Name	Description
Name	Name of the template.
Owner	Specifies the name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template.
Version	Specifies the change version of the template.
Default	Specifies whether the template is default or user-defined.
Software Version	Specifies the software version of the element for the template.
Last Modified	Specifies the time and date when the template was last modified.

Messaging template

Name	Description
Name	Name of the template.

Name	Description
Owner	Specifies the name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template.
Version	Specifies the change version of the template.
Default	Specifies whether the template is default or user-defined.
Type	Specifies the type of the messaging template.
Software Version	Specifies the software version of the element for the template.
Last Modified	Specifies the time and date when the template was last modified.

Add Agent Template field descriptions

Field	Description
System Type	Specifies the Communication Manager that the agent is assigned to.
Template Name	Specifies the name of the agent template. You can enter the name of your choice in this field.
Software Version	Specifies the Communication Manager version of the agent template.

Field	Description
AAS	Provides the option to use this extension as a port for an Auto Available Split/Skill. By default, this check box is clear. This option is intended for communication server adjunct equipment ports only, not human agents. **Important:** When you enter y in the AAS field, it clears the password and requires execution of the **`remove agent-loginid`**

Field	Description
	command. To set AAS to n, remove this logical agent, and add it again.
ACW Agent Considered Idle	Provides the option to count After Call Work (ACW) as idle time. The valid entries are **System**, **Yes**, and **No**. Select **Yes** to have agents who are in ACW included in the Most-Idle Agent queue. Select **No** to exclude ACW agents from the queue.
AUDIX	Provides the option to use this extension as a port for AUDIX. By default, this check box is clear. **Note:** The AAS and AUDIX fields cannot both be y.
AUDIX Name for Messaging	You have the following options: • Enter the name of the messaging system used for LWC Reception • Enter the name of the messaging system that provides coverage for this Agent LoginID • Leave the field blank. This is the default setting.
Auto Answer	When using EAS, the auto answer setting of the agent applies to the station where the agent logs in. If the auto answer setting for that station is different, the agent setting overrides the station setting. The valid entries are: • **all**: Immediately sends all ACD and non-ACD calls to the agent. The station is also given a single ring while a non-ACD call is connected. You can use the ringer-off button to prevent the ring when the feature-related system parameter, **Allow Ringer-off with Auto-Answer** is set to y. • **acd**: Only ACD split /skill calls and direct agent calls go to auto answer. If this field is acd, non-ACD calls terminated to the agent ring audibly.

Field	Description
	• **none**: All calls terminated to this agent receive an audible ringing. This is the default setting. • **station**: Auto answer for the agent is controlled by the auto answer field on the Station screen.
Aux Work Reason Code Type	Determines how agents enter reason codes when entering AUX work. The valid entries are: • **system**: Settings assigned on the Feature Related System Parameters screen apply. This is the default setting. • **none**: You do not want an agent to enter a reason code when entering AUX work. • **requested**: You want an agent to enter a reason code when entering AUX mode but do not want to force the agent to do so. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set toy. • **forced**: You want to force an agent to enter a reason code when entering AUX mode. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to y.
Call Handling Preference	Determines which call an agent receives next when calls are in queue. When calls are in queue and an agent becomes available, the following entries are valid: • **skill-level**: Delivers the oldest, highest priority calls waiting for the highest-level agent skill. • **greatest-need**: Delivers the oldest, highest priority calls waiting for any agent skill. • **percent-allocation**: Delivers a call from the skill that will otherwise deviate most from its administered allocation. Percent-allocation is available only with Avaya Business Advocate software.

Field	Description
	For more information, see *Avaya Business Advocate User Guide*.
COR	Specifies the Class Of Restriction for the agent. Valid entries range from **0** to **995**. The default entry is **1**.
Coverage Path	Specifies the coverage path number used by calls to the LoginID. Valid entries are a path number from **1** to **999**, time of day table **t1** to **t999**, or blank (default). This is used when the agent is logged out, busy, or does not answer calls.
Direct Agent Calls First (not shown)	Provides the option to direct agent calls to override the percent-allocation call selection method and be delivered before other ACD calls. Clear the check box if you want to treat direct agent calls as other ACD calls. This field replaces the Service Objective field when percent-allocation is entered in the Call Handling Preference field. For more information, see *Avaya Business Advocate User Guide*.
Direct Agent Skill	Specifies the number of the skill used to handle Direct Agent calls. Valid entries range from **1** to **2000**, or blank. The default setting is blank.
Forced Agent Logout Time	Enables the Forced Agent Logout by Clock Time feature by administering a time of day to automatically log out agents using an hour and minute field. Valid entries for the hour field range from **01** to **23**. Valid entries for the minute field are **00**, **15**, **30**, and **45**. The default is blank (not administered). Examples are: 15:00, 18:15, 20:30, 23:45.
Local Call Preference	Provides the option to administer Local Preference Distribution to handle agent-surplus conditions, call-surplus conditions, or both. Use this field to administer call-surplus conditions. To set up an algorithm for agent-surplus conditions, set the Local Agent Preference field on the Hunt Group screen. You can select this check box only if the Call Center Release field is set to 3.0 or later and the Multiple Locations customer option is active.

Field	Description
LoginID for ISDN/SIP Display	Provides the option to include the Agent LoginID CPN and Name field in ISDN and SIP messaging over network facilities. By default, the check box is clear, indicating that the physical station extension CPN and Name is sent. Send Name on the ISDN Trunk Group screen prevents sending the calling party name and number if set to n and may prevent sending it if set to r (restricted).
Logout Reason Code Type	Determines how agents enter reason codes. The valid entries are: • **System**: Settings assigned on the Feature Related System Parameters screen apply. This is the default entry. • **Requested**: You want an agent to enter a reason code when logging out but do not want to force the agent to do this. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to y. • **Forced**: You want to force an agent to enter a reason code when logging out. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to y. • **None**: You do not want an agent to enter a reason code when logging out.
LWC Reception	Indicates whether the terminal can receive Leave Word Calling (LWC) messages. The valid entries are: • **audix** • **msa-spe**. This is the default entry. • **none**
LWC Log External Calls	Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls provided information on the caller identification is available. Each record consists of the latest call attempt date and time.

Field	Description
Maximum time agent in ACW before logout (Sec)	Sets the maximum time the agent can be in ACW on a per agent basis. The valid entries are: • **system**: This is the default entry. Settings assigned on the Feature Related System Parameters screen apply. • **none**: ACW timeout does not apply to this agent. • **30-9999 sec**: Indicates a specific timeout period. This setting will take precedence over the system setting for maximum time in ACW.
MIA Across Skills	The valid entries are: • **System**: The system-wide values apply. This is the default value. • **Yes**: Removes an agent from the MIA queues for all the splits or skills for which an agent is available when the agent answers a call from any assigned splits or skills. • **No**: Excludes ACW agents for the queue.
Native Name	Specifies the name associated with the agent login ID
Percent Allocation	Specifies the percentage for each of the agent's skills if the call handling preference is percent-allocation. Valid entry is a number from **1** to **100** for each skill. Entries for all the agent skills together must add up to 100%. Do not use target allocations for reserve skills. Percent Allocation is available as part of the Avaya Business Advocate software.
Password	Specifies the password the agent must enter upon login. Displayed only if both the AAS and AUDIX check boxes are clear. Valid entries are digits from **0** through **9**. Enter the minimum number of digits in this field specified by the Minimum Agent-LoginID Password Length field on the Feature-Related System Parameters screen. By default, this field is blank.
Confirm Password	Confirms the password the Agent entered in the Password field during login. Displayed only if both the AAS and the AUDIX check

Field	Description
	boxes are clear. By default, this field is blank. **Note:** Values entered in this field are not echoed to the screen.
Port Extension	Specifies the assigned extension for the AAS or AUDIX port. The values are displayed only if either the AAS or AUDIX check box is selected. This extension cannot be a VDN or an Agent LoginID. By default, this field is blank
Reserve Level	Specifies the reserve level to be assigned to the agent for the skill with the Business Advocate Service Level Supervisor feature or the type of interruption with the Interruptible AUX Work feature. You can assign a reserve level of 1 or 2 or an interruptible level of a, m, n, or blank for no reserve or interruptible level, where, • a: auto-in-interrupt • m: manual-in-interrupt • n: notify-interrupt Changes to this field take effect the next time the agent logs in. Values of 1 and 2 are allowed only if Business Advocate is enabled. A skill level cannot be assigned with a reserve level setting. Reserve level set to 1 or 2 defines the EWT threshold level for the agent to be added to the assigned skill as a reserve agent. When the EWT for this skill reaches the corresponding threshold set on the Hunt Group screen, agents automatically get this skill added to their logged in skills. Agents are delivered calls from this skill until the skill's EWT drops below the assigned overload threshold for that level. The Interruptible Aux feature is a way to help meet service level targets by requesting agents who are on break to become available when the service level target is not being met. For more information on Service Level Supervisor, see *Avaya Business Advocate User Guide*.

Field	Description
Service Objective	Provides the option to administer Service Objective. Service Objective is administered on the Hunt Group screen and the agent LoginID screen. This field is displayed only when Call Handling Preference is set to greatest-need or skill-level. The communication server selects calls for agents according to the ratio of Predicted Wait Time (PWT) or Current Wait Time (CWT) and the administered service objective for the skill. Service Objective is part of the Avaya Business Advocate software.
Security Code	The security code required by users for specific system features and functions, including the following: Personal Station Access, Redirection of Calls Coverage Off-Net, Leave Word Calling, Extended Call Forwarding, Station Lock, Message Retrieval, Terminal Self-Administration, and Demand Printing. The required security code length is administered system-wide.
Skill Number	Specifies the Skill Hunt Groups that an agent handles. The same skill may not be entered twice. You have the following options: • If EAS-PHD is not optioned, enter up to four skills. • If EAS-PHD is optioned, enter up to 20 or 60 skills depending on the platform. **Important:** Assigning a large number of skills to agents can potentially impact system performance. Review system designs with the ATAC when a significant number of agents have greater than 20 skills per agent.
Skill Level	Specifies a skill level for each of an agent's assigned skills. If you specify the EAS-PHD option, 16 priority levels are available. If you do not specify this option, two priority levels are available.
Tenant Number	Specifies the tenant partition number. Valid entries range from **1** to **100**. The default is entry is **1**.

Field	Description
	Note: Values entered in this field are not echoed to the screen.

Button	Description
Commit	Completes the action you initiate.
Clear	Clears all entries.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.

Add Endpoint Template

Endpoint / Template field descriptions

You can use these fields to perform endpoint / template tasks. This page has the exclusive fields that occur for endpoints and templates apart from the **General options**, **Feature Options**, **Site Data**, **Data Module/Analog Adjunct**, **Abbreviated Call Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.

Field description for Endpoints

Name	Description
System	Specifies the Communication Manager that the endpoint is assigned to.
Template	Specifies all the templates that correspond to the set type of the endpoint.
Set Type	Specifies the set type or the model number of the endpoint.
Name	Specifies the name associated with an endpoint. The system displays the name you enter on called telephones that have display capabilities. In some messaging applications, such as Communication Manager Messaging, you enter the user

	name (last name first) and their extension to identify the telephone. The name entered is also used for the integrated directory.

Field description for Templates

Name	Description
Set Type	Specifies the set type or the model of the endpoint template.
Template Name	Specifies the name of the endpoint template. You can enter the name of your choice in this field.

Extension

The extension for this station.

Port

The Auxiliary and Analog ports assigned to the station are as follows.

Valid Entry	Usage
01 to 64	The first and second numbers are the cabinet numbers.
A to E	The third character is the carrier.
01 to 20	The fourth and fifth characters are the slot numbers. G650 has 14 slots.
01 to 32	The sixth and seventh characters are the port numbers.
x or X	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension has a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions.
IP	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have an IP set. This is automatically entered for certain IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.
xxxVmpp	Specifies the Branch Gateway.

Valid Entry	Usage
	• xxx is the Branch Gateway number, which is in the range 001 to 250. • m is the module number, which is in the range 1 to 9. • pp is the port number, which is in the range 01 to 32.
Analog Trunk port	Analog trunk port is available with: • MM711 and MM714 media modules • TN747 and TN797 circuit packs

General Options

This section lets you set the general fields for a station.

COS

The Class of Service (COS) number used to select allowed features.

Continue on Error

When the system encounters an error, provides an option to continue or abort the implementation of parameter changes.

COR

Class of Restriction (COR) number with the required restriction.

Coverage Path 1 or Coverage Path 2

The coverage-path number or time-of-day table number assigned to the station.

Note:

If Modified Misoperation is active, a Coverage Path must be assigned to all stations on Communication Manager.

TN

Valid Entry	Usage
1 to 100	The Tenant Partition number.

Security Code

The security code required by users for specific system features and functions are as follows:

- Extended User Administration of Redirected Calls
- Personal Station Access
- Redirection of Calls Coverage Off-Net
- Leave Word Calling
- Extended Call Forwarding
- Station Lock

- Voice Message Retrieval
- Terminal Self-Administration
- Enterprise Mobility User
- Extension to Cellular
- Call Forwarding
- Posted Messages
- Security Violation Notification
- Demand Printing

The required security code length is administered system wide.

Emergency Location Ext

The Emergency Location Extension for this station. This extension identifies the street address or nearby location when an emergency call is made. Defaults to the telephone's extension. Accepts up to thirteen digits.

Note:

On the ARS Digit Analysis Table in Communication Manager, 911 must be administered to be call type emer or alrt for the E911 Emergency feature to work properly.

Message Lamp Ext

The extension of the station tracked with the message waiting lamp.

Lock Messages

Controls access to voice messages by other users.

Valid Entry	Usage
y	Restricts other users from reading or canceling the voice messages, or retrieving messages using Voice Message Retrieval.
n	Allows other users to read, cancel, or retrieve messages.

Feature Options

This section lets you set features unique to a particular voice terminal type.

Location

This field appears only when the **Multiple Locations** field on the system parameters customer options screen is set to y and the **Type** field is set to H.323 or SIP station types.

Valid entry	Usage
1 to 250	(Depending on your server configuration, see *Avaya Aura® Communication Manager System Capacities Table*, 03-300511.) Assigns the location number to a particular station. Allows IP telephones

Valid entry	Usage
	and softphones connected through a VPN to be associated with the branch an employee is assigned to. This field is one way to associate a location with a station. For the other ways and for a list of features that use location, see the Location sections in *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.
blank	Indicates that the existing location algorithm applies. By default, the value is blank.

Active Station Ringing

Defines how calls ring to the telephone when it is off-hook without affecting how calls ring at this telephone when the telephone is on-hook.

Valid Entry	Usage
continuous	All calls to this telephone ring continuously.
single	Calls to this telephone receive one ring cycle and then ring silently.
if-busy-single	Calls to this telephone ring continuously when the telephone is off-hook and idle. Calls to this telephone receive one ring cycle and then ring silently when the telephone is off-hook and active.
silent	All calls to this station ring silently.

Auto Answer

In EAS environments, the auto answer setting for the Agent LoginID can override a station's setting when an agent logs in.

Valid Entry	Usage
all	All ACD and non-ACD calls terminated to an idle station cut through immediately. Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when the **Allow Ringer-off with Auto-Answer** is enabled for the system.
acd	Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls terminated to a station ring audibly. For analog stations, the station is off-hook and idle, only the ACD split/ skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the station is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone.
none	All calls terminated to this station receive an audible ringing treatment.
icom	A telephone user can answer an intercom call from the same intercom group without pressing the **intercom** button.

MWI Served User Type

Controls the auditing or interrogation of a served user's message waiting indicator (MWI).

Valid Entries	Usage
fp-mwi	The station is a served user of an fp-mwi message center.
qsig-mwi	The station is a served user of a qsig-mwi message center.
blank	The served user's MWI is not audited or if the user is not a served user of either an fp-mwi or qsig-mwi message center.

Coverage After Forwarding

Governs whether an unanswered forwarded call is provided coverage treatment.

Valid Entry	Usage
y	Coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters.
n	No coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters.
s(ystem)	Administered system-wide coverage parameters determine treatment.

Per Station CPN - Send Calling Number

Determines Calling Party Number (CPN) information sent on outgoing calls from this station.

Valid Entries	Usage
y	All outgoing calls from the station deliver the CPN information as "Presentation Allowed."
n	No CPN information is sent for the call.
r	Outgoing non-DCS network calls from the station delivers the Calling Party Number information as "Presentation Restricted."
blank	The sending of CPN information for calls is controlled by administration on the outgoing trunk group the calls are carried on.

Display Language

Valid Entry	Usage
english french italian spanish user-defined	The language that displays on stations. Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.).
unicode	Displays English messages in a 24-hour format . If no Unicode file is installed, displays messages in English by default. **Note:** Unicode display is only available for Unicode-supported telephones. Currently, 4610SW, 4620SW, 4621SW, 4622SW, 16xx, 96xx, 96x1, and 9600-series telephones (Avaya one-X Deskphone Edition SIP R2

Valid Entry	Usage
	or later) support Unicode display. Unicode is also an option for DP1020 (aka 2420J) and SP1020 (Toshiba SIP Phone) telephones when enabled for the system.

Personalized Ringing Pattern

Defines the personalized ringing pattern for the station. Personalized Ringing allows users of some telephones to have one of 8 ringing patterns for incoming calls. For virtual stations, this field dictates the ringing pattern on its mapped-to physical telephone.

L = 530 Hz, M = 750 Hz, and H = 1060 Hz

Valid Entries	Usage
1	MMM (standard ringing)
2	HHH
3	LLL
4	LHH
5	HHL
6	HLL
7	HLH
8	LHL

Hunt-to Station

The extension the system must hunt to for this telephone when the telephone is busy. You can create a station hunting chain by assigning a hunt-to station to a series of telephones.

Remote Softphone Emergency Calls

Tells Communication Manager how to handle emergency calls from the IP telephone.

⚠ Caution:

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. You cannot use an Avaya IP endpoint to dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. Avoid using an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones.

Available only if the station is an IP Softphone or a remote office station.

Valid Entry	Usage
as-on-local	If the emergency location extension that corresponds to this station's IP address is not administered (left blank), the value as-on-local sends the station emergency location extension to the Public Safety Answering Point (PSAP). If the administrator populates the IP address mapping with emergency numbers, the value as-on-local functions as follows: • If the station emergency location extension is the same as the IP address mapping emergency location extension, the value as-on-local sends the station's own extension to the Public Safety Answering Point (PSAP). • If the station emergency location extension is different from the IP address mapping emergency location extension, the value as-on-local sends the IP address mapping extension to the Public Safety Answering Point (PSAP).
block	Prevents the completion of emergency calls. Use this entry for users who move around but always have a circuit-switched telephone nearby, and for users who are farther away from the server than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP Telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.
cesid	Allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. The end user enters the emergency information into the IP Softphone. Use this entry for IP Softphones with road warrior service that are near enough to the server that an emergency call reaches the PSAP that covers the softphone's physical location. If the server uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the server uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP Softphone location, based on advice from the local emergency response personnel.
option	Allows the user to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported. This entry is used for extensions that can be swapped back and forth between IP Softphones and a telephone with a fixed location. The user chooses between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects the extension.

Service Link Mode

Determines the duration of the service link connection. The service link is the combined hardware and software multimedia connection between an Enhanced mode complex’s H.320 DVC system and a server running Avaya Communication Manager that terminates the H.320 protocol. When the user receives or makes a call during a multimedia or IP Softphone or IP Telephone session, a “service link” is established.

Valid Entry	Usage
as-needed	Used for most multimedia, IP Softphone, or IP Telephone users. Setting the **Service Link Mode** to as-needed leaves the service link connected for 10 seconds after the user ends a call so that they can immediately place or take another call. After 10 seconds, the link is drops. A new link need to be established to place or take another call.
permanent	Used for busy call center agents and other users who are constantly placing or receiving multimedia, IP Softphone, or IP Telephone calls. In permanent mode, the service link stays up for the duration of the multimedia, IP Softphone, or IP Telephone application session.

Loss Group

Valid Entry	Usage
1 to 17	Determines which administered two-party row in the loss plan applies to each station. Is not displayed for stations that do not use loss, such as x-mobile stations and MASI terminals.

Speakerphone

Controls the behavior of speakerphones.

Valid Entry	Usage
1-way	Indicates that the speakerphone listen-only.
2-way	Indicates that the speakerphone is both talk and listen.
grp-listen	With Group Listen, a telephone user can talk and listen to another party with the handset or headset while the telephone's two-way speakerphone is in the listen-only mode. Others in the room can listen, but cannot speak to the other party through the speakerphone. The person talking on the handset acts as the spokesperson for the group. Group Listen provides reduced background noise and improves clarity during a conference call when a group needs to discuss what is being communicated to another party. Available only with 6400-series and 2420/2410 telephones.
none	Not administered for a speakerphone.

LWC Reception

Indicates where Leave Word Calling (LWC) messages are stored.

Valid Entry	Usage
audix	LWC messages are stored on the voice messaging system.
none	LWC messages are not be stored.
spe	LWC messages are stored in the system or on the switch processor element (spe).

Survivable COR

Sets a level of restriction for stations to be used with the survivable dial plan to limit certain users to only to certain types of calls. You can list the restriction levels in order from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by PIM module of the Integrated Management to communicate with the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for Standard Local Survivability (SLS) on the Branch Gateways.

Available for all analog and IP station types.

Valid Entries	Usage
emergency	This station can only be used to place emergency calls.
internal	This station can only make intra-switch calls. This is the default.
local	This station can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.
toll	This station can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables.
unrestricted	This station can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users.

Time of Day Lock Table

Valid Entry	Usage
1 to 5	Assigns the station to a Time of Day (TOD) Lock/Unlock table. The assigned table must be administered and active.
blank	Indicates no TOD Lock/Unlock feature is active. This is the default.

Survivable GK Node Name

Any valid previously-administered IP node name. Identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the Branch Gateways. When a valid IP node name is entered into this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP stations register with Communication Manager, this list is sent down in the registration confirm message. With this, the IP station can use the IP address of this Survivable Gatekeeper as the call controller of last resort.

If blank, there are no external gatekeeper nodes within a customer's network. This is the default value.

Available only if the station type is an H.323 station for the 46*xx* or 96*xx* models.

Media Complex Ext

When used with Multi-media Call Handling, indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to place either a voice or a data call, and voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.

Valid Entry	Usage
A valid BRI data extension	For MMCH, enter the extension of the data module that is part of this multimedia complex.
H.323 station extension	For 4600 series IP Telephones, enter the corresponding H.323 station. For IP Softphone, enter the corresponding H.323 station. If you enter a value in this field, you can register this station for either a road-warrior or telecommuter/Avaya IP Agent application.
blank	Leave this field blank for single-connect IP applications.

AUDIX Name

The voice messaging system associated with the station. Must contain a user-defined adjunct name that was previously administered.

Call Appearance Display Format

Specifies the display format for the station. Bridged call appearances are not affected by this field. This field is available only on telephones that support downloadable call appearance buttons, such as the 2420 and 4620 telephones.

Note:

This field sets the administered display value only for an individual station.

Valid Entry	Usage
loc-param-default	The system uses the administered system-wide default value. This is the default.
inter-location	The system displays the complete extension on downloadable call appearance buttons.
intra-location	The system displays a shortened or abbreviated version of the extension on downloadable call appearance buttons.

IP Phone Group ID

Available only for H.323 station types.

Valid Entry	Usage
0 to 999 blank	The Group ID number for this station.

Always Use

Enables or disables the following emergency call handling settings:

- A softphone can register no matter what emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the administered **Emergency Location Extension** is used. The user-entered settings of the softphone are ignored.
- If an IP telephone dials 911, the administered **Emergency Location Extension** is used.
- If a call center agent dials 911, the physical station extension is displayed, overriding the administered **LoginID for ISDN Display**.

Does not apply to SCCAN wireless telephones, or to extensions administered as type h.323.

Audible Message Waiting

Enables or disables an audible message waiting tone indicating the user has a waiting message consisting of a stutter dial tone when the user goes off-hook.

This field does *not* control the Message Waiting lamp.

Available only if **Audible Message Waiting** is enabled for the system.

Auto Select Any Idle Appearance

Enables or disables automatic selection of any idle appearance for transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Communication Manager selects the first idle appearance.

Bridged Call Alerting

Controls how the user is alerted to incoming calls on a bridged appearance.

Valid Entry	Usage
y	The bridged appearance rings when a call arrives at the primary telephone.
n	The bridged appearance flashes but does not ring when a call arrives at the primary telephone. This is the default. If disabled and **Per Button Ring Control** is also disabled, audible ringing is suppressed for incoming calls on bridged appearances of another telephone's primary extension.

Bridged Idle Line Preference

Specifies whether the selected line for incoming bridged calls is always an idle line.

Valid Entry	Usage
y	The user connects to an idle call appearance instead of the ringing call.
n	The user connects to the ringing call appearance.

CDR Privacy

Enables or disables Call Privacy for each station. With CDR Privacy, digits in the called number field of an outgoing call record can be blanked on a per-station basis. The number of blocked digits is administered system-wide as CDR parameters.

Conf/Trans On Primary Appearance

Enables or disables the forced use of a primary appearance when the held call to be conferenced or transferred is a bridge. This is regardless of the administered value for **Auto Select Any Idle Appearance** .

Coverage Msg Retrieval

Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.

IP Video

Enables or disables IP video capability for this signaling group. Available only if the signaling group type h.323 and sip.

Data Restriction

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

Direct IP-IP Audio Connections

Supports or prohibits direct audio connections between IP endpoints that saves on bandwidth resources and improves sound quality of voice over IP transmissions.

Display Client Redirection

Enables or disables the display of redirection information for a call originating from a station with Client Room Class of Service and terminating to this station. When disabled, only the client name and extension or room display. Available only if Hospitality is enabled for the system.

Note:

This field must be enabled for stations administered for any type of voice messaging that needs display information.

Select Last Used Appearance

Valid Entry	Usage
y	Indicates a station's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. The line selection on an on-hook station only moves from the last used line button to a line button with an audibly alerting call. If there are no alerting calls, the line selection remains on the button last used for a call.
n	The line selection on an on-hook station with no alerting calls can be moved to a different line button that might be serving a different extension.

Survivable Trunk Dest

Designates certain telephones as not being allowed to receive incoming trunk calls when the Branch Gateway is in survivable mode. This field is used by the PIM module of the Integrated Management to successfully interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the Branch Gateways.

Available for all analog and IP station types.

Valid Entry	Usage
y	Allows this station to be an incoming trunk destination while the Branch Gateway is running in survivability mode. This is the default.
n	Prevents this station from receiving incoming trunk calls when in survivable mode.

H.320 Conversion

Enables or disables the conversion of H.320 compliant calls made to this telephone to voice-only. The system can handle only a limited number of conversion calls. Therefore, the number of telephones with H.320 conversion must be limited.

Idle Appearance Preference

Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.

Valid Entry	Usage
y	The user connects to an idle call appearance instead of the ringing call.
n	The Alerting Appearance Preference is set and the user connects to the ringing call appearance.

IP Audio Hairpinning

Enables or disables hairpinning for H.323 or SIP trunk groups. H.323 and SES-enabled endpoints are connected through the IP circuit pack without going through the time division multiplexing (TDM) bus. Available only if **Group Type** is h.323 or sip.

IP Softphone

Indicates whether or not this extension is either a PC-based multifunction station or part of a telecommuter complex with a call-back audio connection.

Available only for DCP station types and IP Telephones.

LWC Activation

Activates or deactivates the Leave Word Calling (LWC) feature. With LWC, internal telephone users on this extension can leave short pre-programmed messages for other internal users.

You must use LWC if:

- The system has hospitality and the guest-room telephones require LWC messages indicating that wakeup calls failed
- The LWC messages are stored in a voice-messaging system

LWC Log External Calls

Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls provided information on the caller identification is available. Each record consists of the latest call attempt date and time.

Multimedia Early Answer

Enables or disables multimedia early answer on a station-by-station basis.

You must enable the station for the Multimedia Early Answer feature if the station receives coverage calls for multimedia complexes, but is not multimedia-capable. This ensures that calls are converted and the talk path is established before ringing at this station.

Mute Button Enabled

Enables or disables the mute button on the station.

Per Button Ring Control

Enables or disables per button ring control by the station user.

Valid Entries	Usage
y	Users can select ring behavior individually for each call-appr, brdg-appr, or abrdg-appr on the station and to enable Automatic Abbreviated and Delayed ring transition for each call-appr on the station. Prevents the system from automatically moving the line selection to a silently alerting call unless that call was audibly ringing earlier.
n	Calls on **call-appr** buttons always ring the station and calls on **brdg-appr** or **abrdg-appr** buttons always ring or not ring based on the **Bridged Call Alerting** value. The system can move line selection to a silently alerting call if there is no call audibly ringing the station.

Precedence Call Waiting

Activates or deactivates Precedence Call Waiting for this station.

Redirect Notification

Enables or disables redirection notification that gives a half ring at this telephone when calls to this extension are redirected through Call Forwarding or Call Coverage. Must be enabled if LWC messages are stored on a voice-messaging system.

Restrict Last Appearance

Valid Entries	Usage
y	Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only.
n	Last idle call appearance is used for incoming priority calls and outgoing call originations.

EMU Login Allowed

Enables or disables using the station as a visited station by an Enterprise Mobility User (EMU).

Bridged Appearance Origination Restriction

Restricts or allows call origination on the bridged appearance.

Valid Entry	Usage
y	Call origination on the bridged appearance is restricted.
n	Call origination ion the bridged appearance is allowed. This is normal behavior, and is the default.

Voice Mail Number

Displays the complete voice mail dial up number. Accepts a value of up to 24 characters consisting of digits from 0 to 9, asterisk (*), pound sign (#), ~p (pause), ~w/~W (wait), ~m (mark), and ~s (suppress). This field is supported in the following set types: 9620SIP, 9630SIP, 9640SIP, 9650SIP, 9608SIP, 9611SIP, 9621SIP, 9641SIP, 9608SIPCC, 9611SIPCC, 9621SIPCC, and 9641SIPCC.

Site Data

This section lets you set information about the Room, Floor, Jack, Cable, Mounting, and Building.

Room

Valid Entry	Usage
Telephone location	Identifies the telephone location. Accepts up to 10 characters.
Guest room number	Identifies the guest room number if this station is one of several to be assigned a guest room and the **Display Room Information in Call Display** is enabled for the system. Accepts up to five digits.

Floor

A valid floor location.

Jack

Alpha-numeric identification of the jack used for this station.

Cable

Identifies the cable that connects the telephone jack to the system.

Mounting

Indicates whether the station mounting is d(esk) or w(all).

Building

A valid building location.

Set Color

Indicates the set color. Valid entries include the following colors: beige, black, blue, brown, burg (burgundy), gray, green, ivory, orng (orange), red, teak, wal (walnut), white, and yel (yellow).

You can change the list of allowed set colors by using the Valid Set Color fields on the site-data screen.

Cord Length

The length of the cord attached to the receiver. This is a free-form entry, and can be in any measurement units.

Headset

Indicates whether or not the telephone has a headset.

Speaker

Indicates whether or not the station is equipped with a speaker.

Abbreviated Call Dialing

This section lets you create abbreviated dialing lists for a specific station, and provide lists of stored numbers that can be accessed to place local, long-distance, and international calls; allows you to activate features or access remote computer equipment and select enhanced, personal, system or group lists.

Abbreviated Dialing List 1, List 2, List 3

Assigns up to three abbreviated dialing lists to each telephone.

Valid Entry	Usage
enhanced	Telephone user can access the enhanced system abbreviated dialing list.
group	Telephone user can access the specified group abbreviated dialing list. Requires administration of a group number.
personal	Telephone user can access and program their personal abbreviated dialing list. Requires administration of a personal list number.
system	Telephone user can access the system abbreviated dialing list.

Personal List

Establishes a personal dialing list for telephone or data module users. The personal list must first be assigned to the telephone by the System Administrator before the telephone user can add entries in the list. Users access the lists to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Abbreviated Dialing Enhanced List

Establishes system-wide or personal lists for speed dialing.

The Enhanced Abbreviated Dialing List can be accessed by users to place local, long-distance, and international calls; to activate or deactivate features; or to access remote computer equipment.

Note:

Dialing must be activated in the license file before the Enhanced List can be programmed.

Group List

Implements the Abbreviated Dialing Group List. The System Administrator controls the Group Lists. Up to 100 numbers can be entered for every group list. Users can access this list to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Enhanced Call Fwd

This section allows you to specify the destination extension for the different types of call forwards.

Forwarded Destination

A destination extension for both internal and external calls for each of the three types of enhanced call forwarding (Unconditional, Busy, and No Reply). Accepts up to 18 digits. The first digit can be an asterisk *.

Requires administration to indicate whether the specific destination is active (enabled) or inactive (disabled).

SAC/CF Override

With **SAC/CF Override**, the user of a station with a **Team** button administered, who is monitoring another station, can directly reach the monitored station by pushing the **Team** button. This overrides any currently active rerouting, such as Send All Calls and Call Forwarding, on the monitored station.

Valid Entries	Usage
Ask	The system asks if the user wants to follow the rerouting or override it. When the user has the option to decide whether rerouting must take place or not, a message is sent to the station that displays the active rerouting and the number of the forwarded to station.
No	Cannot override rerouting. The station does not have the ability to override the rerouting of a monitored station.
Yes	Can override rerouting. The station can override the rerouting the monitored station has set, as long as one incoming call appearance is free.

Button Assignment

This section lets you assign features to the buttons on a phone. You can assign the main buttons for your station by choosing an option from the list down box for each button.

Group Membership

This section describes the different groups that an extension can be a member of. Select the station you want to group, and then choose the group from the drop-down box, before you click **Commit**.

Understanding groups

Your voice system uses groups for a number of different purposes. This topic describes the different groups that an extension can be a member of. However, your voice system might include other types of groups such as trunk groups. For more information on groups, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Your voice system can have any of the following types of groups set up:

Type	Description
group page	Group page is a feature that allows you to make an announcement to a pre-programmed group of phone users. The announcement is heard through the speakerphone built into some sets. Users will hear the announcement if their set is idle. Users cannot respond to the announcement.
coverage answer group	A coverage answer group lets up to 8 phones ring simultaneously when a call is redirected to the group.
coverage path	A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call.

Type	Description
	For more information on coverage paths, see “Creating Coverage Paths” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
hunt group	A hunt group is a group of extensions that receive calls according to the call distribution method you choose. When a call is made to a certain phone number, the system connects the call to an extension in the group. Use hunt groups when you want more than one person to be able to answer calls to the same number. For more information on hunt groups, see “Managing Hunt Groups” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
intercom group	An intercom group is a group of extensions that can call each other using the intercom feature. With the intercom feature, you can allow one user to call another user in a predefined group just by pressing a couple of buttons. For more information on intercom groups, see “Using Phones as Intercoms” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
pickup group	A pickup group is a group of extensions in which one person can pick up calls of another person. For more information on pickup groups, see “Adding Call Pickup” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
terminating extension group	A Terminating Extension Group (TEG) allows an incoming call to ring as many as 4 phones at one time. Any user in the group can answer the call. For more information on terminating extension groups, see “Assigning a Terminating Extension Group” in the *Administering Avaya Aura® Communication Manager, 03-300509*.

Subscriber Messaging Templates field descriptions

Field	Description
Template name	Specifies the template of this subscriber template.
Type	Specifies the messaging type of the subscriber template.
Software Version	Specifies the software version of the element for the template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
PBX Extension	Specifies a number whose length can range from three digits to 10 digits, that the subscriber will use to log on to the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local computer.
Password	The default password that a user has to use to log on to his or her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank
Class Of Service	The Class Of Service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down list.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving

Field	Description
	among groups of subscribers. The default value is 1.

Subscriber Directory

Field	Description
Telephone Number	Specifies the name that the system displays before the computer name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.
ASCII version of name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Mailbox Features

Field	Description
Personal Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses `0` while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent

Field	Description
	messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, callers can page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
VoiceMail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: use this to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Miscellaneous1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Reset or **Clear**	Undoes all the changes.
Edit	Allows you to edit the fields.
Done	Completes your action and takes you to the previous page.
Cancel	Takes you to the previous page.
Schedule	Performs the action at the chosen time.

Subscriber CMM Templates field descriptions

Field	Description
Template name	Specifies the template of this subscriber template.
New Template Name	Specifies the name of the duplicate template. You can enter the name of your choice.
Type	Specifies the messaging type of the subscriber template.

Field	Description
Software Version	Specifies the software version of the element for the template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local computer.
Password	The default password that a user has to use to login to his or her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank. • Leave this field blank if you must use the host switch number. • Enter **0** if no message waiting indicators must be sent for this subscriber. You must

Field	Description
	enter 0 when the subscriber does not have a telephone on any switch in the network.
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that the system displays before the computer name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Reset or **Clear**	Undoes all the changes.
Edit	Allows you to edit the fields.
Done	Completes your action and takes you to the previous page.
Cancel	Takes you to the previous page.

Subscriber MM Templates field descriptions

Field	Description
Type	Specifies the messaging type of the subscriber template.
New Template Name	Specifies the name of the duplicate template. You can enter the name of your choice.
Template name	Specifies the messaging template of a subscriber template.

Field	Description
Software Version	Specifies the software version of the element for the template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
Class Of Service	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that the system displays before the computer name and domain in the subscriber's e-mail address. The computer name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen

Field	Description
	(-), plus sign (+), and left and right parentheses ([) and (]) .
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent

Field	Description
	messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, callers can page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: use this to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Reset	Undoes all the changes.
Edit	Allows you to edit the fields.
Done	Completes your action and takes you to the previous page.
Cancel	Takes you to the previous page.

Managing B5800 Endpoint template

Adding a B5800 Endpoint template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 Endpoint**.
3. Under **B5800 Branch Gateway Endpoint Templates**, click **New**.

4. Enter the required information in the **Name**, **System Type**, **Set Type**, and **Version** fields.
5. Click the **Details** button. This action launches the B5800 Branch Gateway Manager application.
6. On the B5800 Branch Gateway Manager window, specify the required details, such as voice mail, telephony, and button programming under the respective tabs on the right pane.
7. Click **File** > **Save Template and Exit** to save the template configuration and exit the B5800 Branch Gateway application. The system directs you to the landing page of **B5800 Endpoint**.

   You can view the newly created template in the list of templates under B5800 Branch Gateway Endpoint Templates.

Related topics:

B5800 Endpoint template field descriptions on page 941

Viewing a B5800 Endpoint template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 Endpoint**.
3. Select a type of system from the list of B5800 Branch Gateway Supported Templates.
4. Click **Show List**.
5. Under **B5800 Branch Gateway Endpoint Templates**, select the template you want to view from the list of templates.
6. Click **View**.
   This action launches the B5800 Branch Gateway Manager application.
7. On the Avaya B5800 Branch Gateway Manager window, click the tabs on the right pane to view the template details.
8. Click **File** > **Exit** to exit the B5800 Branch Gateway Manager application.
   The system directs you to the landing page of **B5800 Endpoint**.

Related topics:

B5800 Endpoint template field descriptions on page 941

Editing a B5800 Endpoint template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 Endpoint**.
3. Select a type of system from the list of B5800 Branch Gateway Supported Templates.
4. Click **Show List**.
5. From the list of **B5800 Branch Gateway Endpoint Templates**, select the template you want to edit.
6. Click **Edit**.

   This action launches the B5800 Branch Gateway application.
7. On the Avaya B5800 Branch Gateway Manager window, edit the required details provided under the tabs on the right pane.
8. Click **File** > **Save Template and Exit** to save the modifications to the template and exit the Avaya B5800 Branch Gateway Manager application.
   The system directs you to the B5800 Endpoint landing page.

Related topics:

B5800 Endpoint template field descriptions on page 941

Duplicating a B5800 endpoint template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 Endpoint**.
3. Select a system type from the list of B5800 Branch Gateway Supported Templates.
4. Click **Show List**.
5. From the list of B5800 Branch Gateway Endpoint Templates, select the template you want to duplicate.
6. Click **Duplicate**.
7. Type a template name in the **New Template Name** field.

8. Click **Commit**.
   If you want to make changes to the new endpoint template, click **Details**.

Related topics:

B5800 Endpoint template field descriptions on page 941

Deleting a B5800 Endpoint template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 Endpoint**.
3. Select a type of system from the list of B5800 Branch Gateway Supported Templates.
4. Click **Show List**.
5. Under **B5800 Branch Gateway Endpoint Templates**, select the template you want to delete from the list of templates.
6. Click **Delete**. The system displays the template instance you selected for deletion.
7. Perform one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation and return to the **B5800 Endpoint** landing page.

B5800 Endpoint template field descriptions

Name	Description
Name	Displays the name of the B5800 Endpoint template.
System Type	Displays the type of system associated with the B5800 Branch Gateway device. The valid options are: • **B5800**: for Core Unit • **B5800L**: for Linux systems

Name	Description
Version	Displays the version of the B5800 endpoint template.
Set Type	Displays the set type associated with the B5800 Endpoint template. This is a drop-down field listing the following set types: • **ANALOG** • **SIP** • **IPDECT** • **DIGITAL** • **H323** For Linux devices, only **SIP**, **IPDECT**, and **H323** are supported.
Last Modified Time	Displays the date and time when you last modified the template.

Button	Description
Details	Opens the B5800 Branch Gateway application to add or edit the template details.

Managing B5800 System Configuration template

Adding a B5800 System Configuration template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 System Configuration**.
3. Under **B5800 Branch Gateway System Configuration**, click **New**.
4. Complete the **Name**, **System Type**, and **Version** fields.
5. Click **Details**. This action launches the B5800 Branch Gateway application.
6. On the Offline Configuration Creation window, click **OK**.
7. Complete the system configuration template by filling up the required fields under the tabs on the right pane and click **OK**.

8. Click **File** > **Save Template and Exit** to save the template specifications and exit theB5800 Branch Gateway application.

   The system directs you to the B5800 System Configuration landing page where you can view the newly created system template in the B5800 Branch Gateway System Configuration list.

Related topics:

B5800 System Configuration template field descriptions on page 945

Viewing a B5800 System Configuration template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 System Configuration**.
3. On the B5800 Branch Gateway Template page, select a B5800 Branch Gateway system type from the B5800 Branch Gateway Supported Templates list.
4. Click **Show List**.
5. Select the system configuration template you want to view from the B5800 Branch Gateway System Configuration list.
6. Click **View**. This action launches the B5800 Branch Gateway Manager application.
7. On the Avaya B5800 Branch Gateway Manager window, you can view the system configuration template details under the various tabs on the right pane. All fields are view only.
8. Click **File** > **Exit** to exit B5800 Branch Gateway Manager.
   The system directs you to the B5800 System Configuration landing page.

Related topics:

B5800 System Configuration template field descriptions on page 945

Editing a B5800 System Configuration template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 System Configuration**.

3. On the B5800 Branch Gateway Template page, select a B5800 Branch Gateway system type from the B5800 Branch Gateway Supported Templates list.
4. Click **Show List**.
5. Select the system configuration template you want to edit from the B5800 Branch Gateway System Configuration list.
6. Click **Edit**.

   This action launches the Avaya B5800 Branch Gateway Manager application.
7. On the Avaya B5800 Branch Gateway Manager window, edit the required configuration parameters under the various tabs on the right pane and click **OK**.
8. Click **File** > **Save Template and Exit** to save the modifications to the system configuration template and exit theB5800 Branch Gateway Manager application.

   The system directs you to the B5800 System Configuration landing page.

Related topics:

B5800 System Configuration template field descriptions on page 945

Deleting a B5800 System Configuration template

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 System Configuration**.
3. On the B5800 Branch Gateway Template page, select a B5800 Branch Gateway system type from the B5800 Branch Gateway Supported Templates list.
4. Click **Show List**.
5. Select the system configuration template you want to delete from the B5800 Branch Gateway System Configuration list.
6. Click **Delete**.
7. The system displays the system template instance you selected for deletion. Perform one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation and return to the B5800 System Configuration landing page.

Related topics:

B5800 System Configuration template field descriptions on page 945

Applying a B5800 System Configuration template on a B5800 Branch Gateway device

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 System Configuration**.
3. On the B5800 Branch Gateway Template page, select a B5800 Branch Gateway system type from the B5800 Branch Gateway Supported Templates list.
4. Click **Show List**.
5. From the B5800 Branch Gateway System Configuration List, select the system template you want to apply to a B5800 Branch Gateway device.
6. Click **Apply**.

   You will be directed to a new page where you can select a device to apply the template.
7. From the list of B5800 Branch Gateway devices, select the B5800 Branch Gateway device on which you want to apply the selected B5800 system configuration template.

   Important:

   When you apply a template on a device, the data of the template that you wish to apply may override the existing system configuration data on the device.
8. Click **Now** to perform apply the template immediately or perform one of the following:
   - Click **Schedule** to apply the template at a specified time in **Scheduler**.
   - Click **Cancel** to cancel this task and return to the B5800 System Configuration landing page.

Related topics:

B5800 System Configuration template field descriptions on page 945

B5800 System Configuration template field descriptions

Name	Description
Name	Displays the name of the B5800 System Configuration template.

Name	Description
System Type	Displays the type of system associated with the template. The valid options are **B5800** and **B5800 for Linux**.
Version	Displays the version number of the template.
Last Modified Time	Displays the date and time you last modified the B5800 System Configuration template.
Details button	Opens the B5800 Branch Gateway application to add or edit the template details.

Manage audio files

Audio files in .WAV and .C11 formats are used in auto attendant configuration in the Auto Attendant feature in B5800 Branch Gateway. In System Manager, you can manage .WAV and .C11 audio files from the Manage Audio page in B5800 System Configuration in Template Management. The .C11 audio file is for use in B5800 Branch Gateway IP500V2 or B5800 Core Unit and the .WAV audio file for B5800 Branch Gateway Linux systems.

To push an auto attendant file to a B5800 System Configuration template through System Manager, you must first upload the .WAV audio files using the **Upload** button in the Manage Audio page. When you upload the .WAV audio files, the corresponding .C11 audio files are automatically created. If you need to convert any .WAV audio file which does not have a corresponding .C11 audio file, or if the corresponding .C11 audio file is deleted, click the **Convert** button in the Manage Audio page.

Use the **Manage Audio** page in **B5800 System Configuration** to:

- Upload .WAV and .C11 audio files.
- Convert .WAV to .C11 audio file format.
- Delete .WAV and .C11 audio files.

Uploading an audio file

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 System Configuration**.
3. Under **B5800 Branch Gateway System Configuration**, click **More Options** > **Manage Audio**.

4. On the Manage Audio page, enter the complete path of the audio file in the **Select an Audio File** text box. You can also click the **Browse** button to locate and select the audio file you want to upload.
5. The system displays the audio file you selected for uploading in a table. If you want to remove the audio file from your selection, click the **Remove** link under the **Action** column.
6. Click **Upload**.

   You can view the newly uploaded audio files listed in the **List of Audio Files** table.

Related topics:

Manage Audio field descriptions on page 948

Converting .WAV to .C11 audio file format

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 System Configuration**.
3. Under **B5800 Branch Gateway System Configuration**, click **More Options** > **Manage Audio**.
4. On the Manage Audio page, select the .WAV audio file from the **List of Audio Files** that you want to convert to .C11 format.
5. On the Convert Audio page, the system lists the file you selected for conversion.
6. If you want to change the recording label of the .WAV file, edit the label text in the corresponding text box under the **Recording Label** column.
7. Click **Commit** to confirm the convert action.

   The system displays the newly converted audio file under the corresponding audio name column in the **List of Audio Files** table.

Related topics:

Manage Audio field descriptions on page 948

Deleting an audio file

About this task

Use the **Delete** button to delete audio files from the List of Audio Files. You can choose to delete either the .WAV or .C11 audio file format, or delete both the audio file formats in a single step.

Procedure

1. On the System Manager Web Console, click **Services** > **Templates**.
2. In the left navigation pane, click **B5800 System Configuration**.
3. From **B5800 Branch Gateway System Configuration**, click **More Options** > **Manage Audio**.
4. On the Manage Audio page, select the audio file you want to delete from the List of Audio Files.
5. Click **Delete**.
6. On the Delete Audio File Confirmation page, you can view the audio files you selected in Step 4 for deletion. From the **Select the type of deletion** field perform one of the following:
   - Select the type of audio file extension you want to delete.
   - Select **Both** if you want to delete both the file extension types.

   Sample scenario: Suppose you have ABC.wav and ABC.c11 audio files in the **List of Audio Files**. If you want to delete only the ABC.wav audio file, then select **Wave** under **Select the type of deletion**. If you want to delete both the audio files in a single step, then select **Both** from the **Select the type of deletion** field.
7. Click **Delete**.
8. Click **Done** to return to the B5800 System Configuration landing page.

Related topics:

Manage Audio field descriptions on page 948

Manage Audio field descriptions

Name	Description
wav Audio File Name	Displays the file name of the .WAV type of audio file.

Name	Description
Last uploaded time of wav	Displays the time when you last uploaded the .WAV audio file in the system.
Recording Label	Displays the recording label of the .wav file.
C11 Audio File Name	Displays the file name of the .C11 type of audio file.
Last converted time of wav to C11	Displays the time when you last converted the.wav file to a .C11 audio file.
Select an Audio File	Displays the complete path of the audio file.
Select the type of deletion on the Delete Audio File Confirmation page	Provides the option to select the type of deletion of audio files. The valid options are: • **Wave**: Deletes only the .WAV type of file for the selected audio file. • **C11**: Deletes the only the .C11 type of file for the selected audio file.. • **Both**: Deletes both, .WAV and .C11, types of files for the selected audio file.

Button	Description
Delete	Deletes the selected audio file.
Convert	Converts an audio file of type .WAV to .C11.
Done	Exits the **Manage Audio** page and return to the B5800 Branch Gateway Template List page.
Browse	To locate and select an audio file.
Upload	Uploads an audio file to System Manager.
Delete on the Delete Audio File Confirmation page	Confirms the delete action for the selected audio file.
Cancel on the Delete Audio File Confirmation page	Cancels the delete operation and returns you to the **Manage Audio** page.

Chapter 14: Security

Managing certificates

About Trust Management

System Manager uses Trust Management to provision and manage certificates of various applications, servers, and devices thereby enabling a secure, inter-element communication. Trust Management provides Identity (Server) and Trusted (Root/CA) certificates that applications can use to establish mutually authenticated TLS sessions.

System Manager uses a third-party open source application, Enterprise Java Beans Certificate Authority (EJBCA), as a Certificate Authority for certificate management.

Trust Management updates for release 6.2

For the 6.2 release, you can manage certificates for System Manager and Unified Communications Management (UCM) through two independent user interface. Go to **Elements** > **Inventory** in the System Manager home page to manage certificates for System Manager and its Managed Elements.

For UCM and its Managed Elements, use **Administrators** > **Certificates** to manage the certificates.

Related topics:

Certificate Authorities on page 956

Setting enrollment password

About this task

You can use this functionality to generate the enrollment password for managed elements. The managed elements require the enrollment password to request certificates from the System Manager Trust Management.

Procedure

1. On the System Manager Web Console, click **Services** > **Security**.

2. In the left navigation pane, click **Certificates** > **Enrollment Password**.
3. On the Enrollment Password page, select the expiration of password in hours in the **Password expires in** field.
4. Enter a password in the **Password** field.
   If you want the system to generate the password, leave the **Password** field blank, and click **Generate**.
5. Click **Commit**.
   The time displayed next to the **Time remaining** label is updated by the value selected in the **Password expires in** field.

Related topics:

Enrollment Password field descriptions on page 958

Adding trusted certificates

About this task

You need to import the certificates that you want to add as trusted certificate in the trust store of the application. The following are the four methods of importing a trusted certificate in the trust store for an application instance:

1. Import from existing
2. Import from file
3. Import as PEM Certificate
4. Import using TLS

You can add a trusted certificate from a list of an existing certificates, a file, a remote location using TLS connection, and by copying the content from a PEM file.

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an application and click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **Add**.
5. On the Add Trusted Certificate page, select store type from the **Store Type** field and perform one of the following steps:
   - To import certificates from existing certificates:
     i. Click **Import from existing** .

ii. Select the certificate from the Global Trusted Certificate section.

iii. Click **Commit**.

- To import certificates from a file:

i. Click **Import from file** .

ii. Enter the name of the file. You can also click **Browse** to select a file.

iii. Click **Retrieve Certificate**.

iv. Click **Commit**.

- To import certificates in the PEM format:

i. Locate the PEM certificate.

ii. Open the certificate in the Notepad application.

iii. Select all the contents in the file.

iv. Perform a copy operation.

v. Click **Import as PEM Certificate**.

vi. Perform a paste operation in the box provided at the bottom of the page.

Note:

You may include the start and end tags:“ -----BEGIN CERTIFICATE-----” and“ -----END CERTIFICATE----”.

vii. Click **Commit**.

- To import using TLS:

i. Click **Import using TLS** .

ii. Enter the IP address of the computer in the **IP Address** field.

iii. Enter the port of the computer in the **Port** field.

iv. Click **Retrieve Certificate**.

v. Click **Commit**.

Related topics:

Adding a UCM CA certificate to a System Manager managed element trusted certificate list on page 957

Add Trusted Certificate field descriptions on page 960

Viewing trusted certificates

About this task

Allows you to view the trusted certificates of System Manager and its managed elements.

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an application and click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **View**.
   The View Trust Certificate page displays the details of the selected certificate.

Related topics:

View Trust Certificate field descriptions on page 962

Removing trusted certificates

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page , select an application and click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, select the certificates you want to remove.
5. Click **Remove**.
   Trust Management removes the certificates from the list of trusted certificates for the application you selected.

Viewing identity certificates

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.

2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an application and click **More Actions** > **Configure Identity Certificates**.
   The Identity Certificate page displays the identity certificates for the application you selected.

Related topics:

Identity Certificates field descriptions on page 964

Replacing an identity certificate

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an application and click **More Actions** > **Configure Identity Certificates**.
4. On the Identity Certificates page, select the certificate you want to replace.
5. Click **Replace**.
6. On the Replace Identity Certificate page, perform one of the following steps:
   - Click **Replace this Certificate with Internal CA Signed Certificate** and do the following:
     - Enter the common name.
     - Select key size and key algorithm from the respective field.
     - Click **Commit** to replace the identity certificate with the internal CA signed certificate.
   - Click **Import third party PCKS # 12 file** and do the following:
     - Enter the file name in the **Please select a file** field.
     - Enter the password in the **Password** field.
     - Click **Retrieve Certificate**. The Certificate Details section displays the details of the certificate.
     - Click **Commit** to replace the certificate with the imported third-party certificate.

Related topics:

Replace Identity Certificate field descriptions on page 964

Renewing identity certificates

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an application and click **More Actions** > **Configure Identity Certificates**.
4. On the Identity Certificates page, select the certificate you want to renew.
5. Click **Renew**.

Certificate Authorities

As a part of the System Manager 6.2 release, Trust Management supports two Certificate Authorities. One for System Manager and its managed elements, and the other for UCM and its managed elements. Thus System Manager 6.2 supports two independent user interfaces for Certificate Authority.

In System Manager, element installation sets up the trust between System Manager and its managed elements. Similarly, UCM has a trust management process to set up the trust between UCM and its managed elements. To enable the UCM managed elements to be in the same trust domain as the System Manager managed elements, you should import the UCM Certificate Authority (CA) certificate to the System Manager managed element's trusted certificate list. Also, import the System Manager CA certificate to UCM managed element's trusted certificate list.

Through the following tasks you can import the UCM certificate to the System Manager managed element's list of trusted certificates and import the System Manager CA certificate to the UCM managed element's trusted certificate list.

Retrieving the UCM CA certificate on page 957

Adding a UCM CA certificate to a SMGR managed element trusted certificate list on page 957

Retrieving the CA certificate on page 958

Retrieving the UCM CA certificate

Procedure

1. On the System Manager console, click **Users** > **Administrators**.
2. On the UCM cut through, click **Certificates** from the left navigation pane.
3. Click the **Private Certificate Authority** tab.
4. Click **Download**.
   The system generates a .cer file. Save it to your local system.

Adding a UCM CA certificate to a System Manager managed element trusted certificate list

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. In the **Elements** section, select a managed element instance.
4. Click **More Actions** > **Configure Trusted Certificates**.
   The system displays the certificates that are currently installed on the managed element you selected.
5. To add a UCM CA certificate, click **Add**.
6. To add the trusted certificate, choose **All** for the Select Store Type .
7. Import the certificate from a file using the **Import from file** option.
8. To select a file, click **Browse**.
9. Before you continue, click **Retrieve Certificate** and review the certificate details.
10. To add the trusted certificate, click **Commit**.

Related topics:

Adding trusted certificates on page 952

Retrieving the System Manager CA certificate

Procedure

1. On the System Manager Web Console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. On the CA Functions page click **Download pem file**.
4. Click **Save** to save the certificate to a file.

Enrollment Password field descriptions

Use this page to generate an enrollment password.

Name	Description
Existing Password	The current enrollment password that the external clients use to request certificates.
Time Remaining	Specifies the time in hours and minutes remaining for expiration of the current password.
Password expires in	Specifies the duration in hours for which the existing password is valid.
Password	The password that the external clients use to request a certificate. Trust Manager generates this password when you click **Generate**.

Button	Description
Generate	Generates a random password.
Commit	Updates the **Existing Password** and **Time Remaining** fields.

Trusted certificate management

Participants in a Public-Key Infrastructure (PKI) scheme use root certification authorities and other intermediate certification authorities to ascertain the trustworthiness of an identity certificate. These certification authorities are collectively known as trust anchors or trusted certificates.

System Manager certificate management supports the following tasks on the trusted certificate of a service:

- Inspect: Trusted Management supports the inspection of each of the trusted certificates that a service use. Additionally, Trusted Management provides details on the subject, issuer, and expiry date of the certificate.
- Add: A service may require to communicate with another service outside the deployment PKI of Aura. For example, for a service to gain access to a remote database or a directory service which presents an identity certificate signed by a commercial CA, include the certificate of the CA in the list of trusted certificates of the service.

  For example, if a service is exposed to multiple SIP endpoints, you cannot add the certificate of the private Certificate Authority (CA) to the trusted certificate store of each client. If each SIP endpoint is configured to trust certificates issued by a commercial CA, then replace the certificate presented by the service with a certificate issued by a commercial CA. Trusted Management supports adding a certificate to a trusted certificate store of the service in the following encodings:

  - ASN.1 DER
  - PEM (OpenSSL)

  Alternatively, you can retrieve a certificate from an SSL socket or from the built-in certificate store.
- Delete: When you do not need a service to participate in an external PKI hierarchy, an administrator can remove the trusted certificate from the trusted certificate store of the service. For example, when the service provider changes, and you do not require the existing service provider.

Trusted Certificates field descriptions

Use this page to view, export, and remove the trusted certificates listed on the page. You can also use this page to add more certificates in the existing list of trusted certificates

Name	Description
Store Description	Specifies the purpose of the trusted certificate.
Store Type	Specifies the type of the store associated with the certificate.
Subject Name	Specifies the name of the certificate holder.

Button	Description
View	Opens the View Trust Certificate page. Use this page to view the certificate details.

Button	Description
Add	Opens the Adds Trusted Certificate page. Use this page to import certificates from the selected resource.
Remove	Removes the selected certificate from the list of trusted certificates.
Exports	Exports the selected certificate from the list of trusted certificates.

Add Trusted Certificate field descriptions

Use this page to add a trusted certificate.

Name	Description
Store Type	Specifies the type of store based on inbound and outbound connection. The options are: • All • TM_INBOUND_TLS • TM_OUTBOUND_TLS • TM_INBOUND_TLS_PEM
Import from existing	Use this option to import a certificate from your local machine.
Import from file	Use this option to import a certificate from a file. The file format is `.cer` or `.crt`.
Import as PEM Certificate	Use this option to import a certificate in .pem format.
Import using TLS	Use this option to import a certificate if the application instance requires to contact the certificate provider to obtain the certificate.

Global Trusted Certificate:

The page displays the following fields when you select the **Import from existing** option.

Name	Description
Certificate Name	Specifies the fully qualified domain name of the certificate.
Subject Name	Specifies the fully qualified domain name of the certificate holder.

Name	Description
Valid To	Specifies the date until which the certificate is valid.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters certificates based on the filter criteria.
Select: All	Select all the certificates in the table.
Select: None	Clears all the check box selections.
Refresh	Refreshes the certificates information .

The page displays these fields when you select the **Import from file** option.

Name/Button	Description
Please select a file	The file that contains the certificates.
Browse	Opens the choose file dialog box. Use this dialog box to choose the file from which you want to import the certificates.
Retrieve Certificate	Retrieves the certificate from the file and displays the details of the certificate in the Certificate Details section.

Certificate Details:

The page displays these fields when you click **Retrieve**.

Name	Description
Subject Details	Specifies the details of the certificate holder.
Valid From	Specifies the date and time from which the certificate is valid.
Valid To	Specifies the date and time until which the certificate is valid.
Key Size	Specifies the size of the key in bits for encryption.

Name	Description
Issuer Name	Specifies the name of the issuer of the certificate.
Finger Print	Specifies the finger print that authenticates the certificate.
CA Certificate	Specifies whether the certificate is a CA certificate.

The page displays these fields when you select the **Import using TLS** option.

Field/Button	Description
IP Address	Specifies the IP address of the certificate provider that is to be contacted for retrieving the certificate.
Port	Specifies the port of the server to be used for obtaining the certificate.
Retrieve Certificate	Retrieves the certificate and displays the details of the certificate in the Certificate Details section.

Related topics:

Adding trusted certificates on page 952

View Trust Certificate field descriptions

Use this page to view details of a selected certificate.

Name	Description
Subject Details	Specifies the details of the certificate holder.
Valid From	Specifies the date and time from which the certificate is valid.
Valid To	Specifies the date and time until which the certificate is valid.
Key Size	Specifies the size of the key in bits for encryption.
Issuer Name	Specifies the name of the issuer of the certificate.
Finger Print	Specifies the finger print that authenticates the certificate.

Button	Description
Done	Closes the page and takes you back to the Trusted Certificates page.

Delete Trusted Certificate Confirmation field descriptions

Use this page to delete a trusted certificate from the list of trusted certificate maintained by the application instance.

Name	Description
Certificate Name	Specifies the common name of the certificate.
Store Type	Specifies the type of the store associated with the certificate.
Subject Name	Specifies the name of the certificate holder.

Button	Description
Delete	Deletes the trusted certificate from the corresponding store.
Cancel	Cancels the delete operation and takes you back to the Add Trusted Certificate page.

Identity certificate management

In Public-Key Infrastructure (PKI), an identity certificate is an electronic document, which uses a digital signature to bind a public key with an identity information such as the name of a person or an organization and address of a person or an organization. The identity certificate is also known as digital certificate or public key certificate. You can use the certificate to verify if a public key belongs to a service.

System Manager supports the following tasks on the identity certificate of a service:

- Inspect: Trusted Management supports inspection of the identity certificate of a service. Additionally, Trusted Management provides details on the subject, issuer, and expiry date of the certificate, and the key size, and key algorithm of the associated key pair.
- Replace: Services that are exposed to external clients may require to present an identity certificate assured by a commercial root CA.

  For example, if a service is exposed to multiple SIP endpoints, you cannot add the certificate of the private Certificate Authority (CA) to the trusted certificate store of each client. If each SIP endpoint is configured to trust certificates issued by a commercial CA,

then replace the certificate presented by the service with a certificate issued by a commercial CA. Also, in protocols like HTTP, the CN value of the certificate must match the host name of the server presenting the certificate. If the host name changes, the subject DN must change.

- Renew: Central administrator may need to reissue an identity certificate that was originally issued by the deployment CA. For example, an identity certificate has a validity date. Therefore, the administrator must replace the certificate before the certificate expires to avoid rejection of the certificate by the service peer.

Identity Certificates field descriptions

Use this page to view the identity certificates for the application instance.

Name	Description
Service Name	Specifies the name of the service that uses the identity certificate.
Common Name	Specifies the common name to identify the service.
Valid To	Specifies the date until which the certificate is valid.
Expired	Specifies whether the certificate has expired or not.
Service Description	A brief description about the service.

Button	Description
Replace	Opens the Replace Identity Certificate page. Use this page to replace a selected identity certificate with a new certificate.
Export	Exports the certificate you select from the table. The exported certificate is in the form of a pem file.
Renew	Renews the certificate you select. After you renew a certificate, the **Valid To** column is automatically updated.

Replace Identity Certificate field descriptions

Use this page to replace an identity certificate.

Certificate Details section

Name	Description
Subject Details	Details of the certificate holder.
Valid From	Specifies the date and time from which the certificate is valid.
Key Size	Specifies the size of the key in bits for encryption.
Issuer Name	Specifies the name of the issuer of the certificate.
Finger Print	Specifies the finger print that authenticates the certificate.
Valid To	Specifies the date and time till the certificate is valid.

Name	Description
Replace this Certificate with Internal CA Signed Certificate	Use this option to replace the current certificate with internal CA signed certificate.
Import third party PCKS #12 file	Use this option if you like to replace the identity certificate with imported third PCKS #12 file.

The page displays following fields when you select **Replace this Certificate with Internal CA Signed Certificate** option.

Name	Description
Common Name (CN):	Specifies the common name of the certificate holder.
Key Algorithm:	Specifies the algorithm used to generate the key for the certificate.
Key Size:	Specifies the size of the key in bits or bytes for encryption.

The page displays following fields when you select **Import third party PCKS #12 file** option.

Name/Button	Description
Please Select a file	The full path of the PKCS #12 file where you have saved the certificate.
Password	The password that is used to retrieve the certificate.

Name/Button	Description
Retrieve Certificate	Retrieves the details of the imported certificate and displays in the following **Certificate Details** section.

Name/Button	Description
Commit	Replaces the current identity certificate with the selected certificate.
Cancel	Cancels the certificate replacement operation.

Related topics:

Replacing an identity certificate on page 955

Using third-party certificate

System Manager supports the use of trusted third-party certificate. You can install and use a third-party certificate in System Manager Web Interface.

Installing and using the third-party certificate for System Manager Web interface involves the following high-level steps:

1. Replacing System Manager Web Server Certificate with third-party certificate.
2. Updating the trust stores for internal services, clients, or managed elements with third-party root and subordinate CA certificate.

For instructions to install the third-party certificate, see “Application notes for supporting third-party certificate in Avaya Aura® System Manager 6.1” on the Avaya Support Web site at http://support.avaya.com.

System Manager Certificate Authority

Setting the System Manager certificate authority (EJBCA) as SUB-CA

About this task

You can use this procedure to change the default Certificate Authority (CA) generated during System Manager installation to an externally signed Sub CA.

Procedure

1. On the System Manager Web Console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **Edit Certificate Authorities**.
4. On the Edit Certificate Authorities page, type the name of your new Sub CA in the text box. For example, ExternalSubCA-1.
5. Click **Create**.
6. On the Create CA page, do the following:
   a. In the **Subject DN** field, enter a DN for your Sub CA. For example, “CN=ExernalSubCA-1,O=AVAYA,C=US”.
   b. In the **Signed By** filed, click `External CA`.
   c. In the **Description** field, provide a description.
7. Click **Make Certificate Request**.

   You must have the CA certificate of the CA that is used to sign the CA. Make sure this certificate is in the PEM format on the same computer on which you have your browser.
8. Click **Choose File** and open the CA certificate file that is in PEM format on you computer.
9. Click **Make Certificate Request**.
   You receive a PEM-formatted certificate request.
10. Click **Download pem file**.
11. Select **Save File** and save the file on your computer.

    You must get the certificate request signed by the CA. If you are using openssl, move the certificate request to the computer where your openssl CA is set up and sign the request.

    Note:

    By default, Openssl reorders the DN to whatever the openssl policy file is set up to do. Use the -preserveDN flag while signing the request using **`openssl ca`** command. Otherwise, the request fails as EJBCA does not recognize the CA.

    Use openssl (openssl x509 –in cert.pem –text) to ensure that the signed request has the X.509 extension **CA:TRUE**.

    Once you get the signed certificate back from the CA in the PEM format, delete any data other than the certificate itself. Ensure that there is no carriage return after the last line.
12. To preserveDN flag, on the linux box, edit `/etc/pki/tls/misc/CA` and search for “-sign|-signreq”.

13. Add preserveDn attribute as: *$CA -policy policy_anything -preserveDN -out newcert.pem -infiles newreq.pem*.
14. On the Linux server, edit `/etc/pki/tls/openssl.cnf`, and change all the occurrences of **basicConstraints=CA:FALSE** to **basicConstraints=CA:TRUE**.

Receiving certificate response

About this task

Ensure that the certificate you have received is properly signed by the CA. You can do this using openssl using **`openssl verify –CAfile ca-cert.pem subca-cert.pem`**

Procedure

1. On the System Manager Web Console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **Edit Certificate Authorities** in the left navigation pane.
4. Select the Sub CA you just created with the “Waiting for Certificate Request” status.
5. Click **Edit**.
6. Select **Receive Certificate Request**.
7. Click **Browse..** to find the signed certificate.
8. Click **Receive Certificate Response**.
   The system displays a message that the certificate response is received successfully, and that the CA is activated. If you do not see this message, double check the contents of the certificate file.

Setting the new CA as the default CA

Procedure

1. On the System Manager Web Console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **Edit Certificate Authorities**.
4. Select the new Sub CA.
   Ensure that the status of the new Sub CA is **Active**.

5. Click **Edit**.
6. Select the **Default CA** check box.
7. Click **Save**.

   This ensures that any request that comes to EJBCA and not specifically referencing the CA by name, use this CA.
8. Select **Edit Certificate Authorities** and highlight “tmdefaultca”.
9. In the text box at the bottom of the page, type in a new name. For example, tmdefaultca-orig.
10. Click **Rename Selected**.

    Important:

    The CRD files refer to tmdefaultca. Therefore, if you do not rename the CA, the requests made to tmdefaultca continue to try using this CA, and fail.

Next steps

After you set the new Sub CA as the default CA, create a backup.

Modifying the default end entities to use the new CA

Procedure

1. On the System Manager Web Console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **Edit Certificate Authorities**.
4. Select **ID_CLIENT**.
5. Click **Edit Certificate Profile**.
6. Go to **Available CAs** and highlight the new Sub CA.
7. Click **Save**.
8. Click **Edit Certificate Profiles** and repeat the Steps 3 through 6 for **ID_CLIENT_SERVER** and **ID_SERVER**.
9. In the left navigation pane, click **Edit End Entity Profiles**.
10. Click **INBOUND_OUTBOUND_TLS**.
11. Click **Edit End Entity Profile**.

    In the **Default CA** field, ensure that you select the new Sub CA.
12. Go to **Available CAs** and highlight the new Sub-CA.
13. Click **Save**.

14. Repeat Steps 8 through 12 for **INBOUND_TLS** and **OUTBOUND_TLS**.
15. Select **List/Edit End Entities** in the left navigation pane.
16. On the List End Entities page, select **All** for the **Or with status** drop down box.
17. Click **List**.
    Verify that the list contains the following three end entities:
    INBOUND_OUTBOUND_TLS, INBOUND_TLS, and OUTBOUND_TLS
18. For each of the end entities, select **Edit End Entity**.
    The system displays a pop-up window.
19. In this pop-up window, ensure that CA is set to your new Sub-CA.
20. Click **Save**.
21. Click **Close**.
22. Click **Reload** located above the end entities
    The system displays your new CA in the **CA** column for all the three entities.

Generating new identity certificates for System Manager

About this task

After CA is set up to issue certificates using the new Sub-CA, update the identity certificates that are created for System Manager during the initialization of System Manager. These certificates are signed by tmdefaultca and not by the new CA. Also, the new CA must be added to the System Manager trust stores.

Procedure

1. On the System Manager Web Console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Enrollment Password**.
3. Fill in the three required fields to set a new Enrollment Password and click **Commit**.

   The system resets the enrollment password, which was lost after the you changed the CA.
4. Start an SSH session on System Manager.
5. Go to `cd /opt/Avaya/Mgmt/6.0.1/trs`, where the installation scripts are located.

   Note:

   The version directory differs.

6. To run the trust initializer script, type `./trust_initializer_install.sh -RMIPORT 1399 -HTTPSPORT 443 -TMCONFIGLOC /opt/Avaya/JBoss/4.2.3/jboss-4.2.3.GA/jboss-as/server/avmgmt/conf/tm`.

   System Manager must have all its identity certificates updated so that they are signed by the new CA, and the new CA must be in the trust stores. Also, you must confirm that this is true.

Confirming identity certificate updates on System Manager

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **System Manager**.
3. On the Manage Elements page, select a System Manager instance and click **More Actions** > **Configure Identity Certificates**.
4. On the Identity Certificates page, select any of the certificates, except weblm_legacy, which is self-signed, and verify that the **Issuer Name** in the window below is the DN of your new CA.

   Note:

   The Issuer Name must not be tmdefaultca.

5. On the Manage Elements page, select a System Manager instance and click **More Actions** > **Configure Trusted Certificates**.

   On the Trusted Certificates page, you must see your new Sub-CA certificate in each of the StoreTypes. You must see three instances on this page.

   Restart all the System Manager applications (JBoss, Apache, stunnel) so that the new certificates are read. Alternatively, you can The easiest way to do this is to reboot the System Manager server.

6. To restart the System Manager applications, reboot the System Manager server.

   The System Manager CA changes from the default, internally generated CA to an externally signed Sub-CA.

External authentication

External authentication

The External Identity Repositories Web page in System Manager contains a summary page for Authentication scheme and Authentication Servers. You can configure the authentication scheme and the authentication servers for System Manager.

System Manager supports up to three authentication authorities:

- local users
- external RADIUS users
- external LDAP users

The authentication scheme policy determines the order that the three authentication authorities are used. The supported order is as follows:

1. local users (default)
2. external RADIUS users then local users
3. external LDAP users then local users
4. external LDAP users, then external RADIUS users, then local users
5. external RADIUS users, then external LDAP users, then local users
6. external KERBEROS server

The authentication servers policy controls the settings for the external LDAP, RADIUS, and KERBEROS servers.

Authentication scheme policy

System Manager supports up to three authentication authorities:

- local servers
- external RADIUS servers
- external LDAP servers (including Sun ONE or Microsoft active directory server)
- KERBREOS server

Editing the authentication scheme

Procedure

1. On the System Manager Web Console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **External Authentication**.
3. On the External Identity Repositories page, click **Edit** in the Authentication Scheme section.
4. On the Authentication Scheme page, select the required authentication scheme.
5. Click **Save**.

Provision the authentication servers

When the LDAP server is Microsoft Active Directory, the full name of the external user must be the same as the logon name that makes the cn attribute of the external users the same as the logon name.

The TCP port used for the external LDAP server and the UDP port used for the external RADIUS server must be open in the Linux iptables firewall, on both the primary security service, and the back up primary security service. To check the status of the iptables rules, use service iptables status.

Provisioning the LDAP server

Procedure

1. On the System Manager Web Console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page complete the **Provision LDAP Server** section.
5. Click **Save**.

Note:

Ensure that the Linux iptable firewall setting, on both the primary and backup security service, allows the TCP port as the source port.

Related topics:

Provision LDAP/Radius/Kerberos server field descriptions on page 975

Provisioning the RADIUS server

Procedure

1. On the System Manager Web Console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page, complete the following information in the Provision RADIUS Server section:
   - **IP (or DNS)**: Type the IP address or DNS name of the primary RADIUS server.
   - **UDP Port**: Type the UDP port number of the primary RADIUS server.
   - **Shared Secret**: Type the shared secret of the RADIUS server.

   Note:

   You must create two records in the external RADIUS server with the same shared secret for both the primary security server and backup security server IP address.
5. Click **Save**.

   Note:

   Ensure the Linux iptable firewall setting on both the primary and backup security service allows the UDP port as the source port.

Related topics:

Provision LDAP/Radius/Kerberos server field descriptions on page 975

Provisioning the Kerberos Server

About this task

Use this functionality to configure the required information for the Kerberos server.

Procedure

1. On the System Manager Web Console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page, complete the following information in the Provision Kerberos Server section:
   - **DC Host Name (FQDN)**: Type your FQDN in the format `machineName.domainName.com/net/`
   - **DC Computer Domain**: Type the domain name of the Kerberos server.
   - **Keytab File**: Type the encrypted Kerberos server key.
5. Click **Save**.

Important:

When logged on to the Kerberos server using Single Sign-on (SSO), you cannot exit from UCM using the Logout link because in this context, SSO automatically authenticates you inside the Domain Controller (DC) domain. You must manually close the browser to exit the application.

Related topics:

Provision LDAP/Radius/Kerberos server field descriptions on page 975

Provision LDAP/Radius/Kerberos server field descriptions

Provision LDAP Server

Name	Description
IP (or DNS)	Specifies the IP address or the DNS name of the LDAP server.
TCP Port	Specifies the TCP port of the LDAP server.

Name	Description
Base Distinguished Name	Specifies the base distinguished name of the LDAP server.
SSL/TLS Mode	Specifies whether the LDAP server supports SSL/TLS connections.
Is Active Directory	Select this check box if active directory does not support anonymous binding.
Supports Anonymous Binding	Select this check box if anonymous binding is supported.
Distinguished Name for Root Binding	Type the distinguished name for the root binding. For example, type cn for Users.
Password for Root Binding	Type the password for the root binding in this field.

Provision Radius Server

Name	Description
IP (or DNS)	Specifies the IP address or the DNS name of the primary RADIUS server.
UDP Port	Specifies the UDP port number of the primary RADIUS server.
Shared Secret	Shared secret of the RADIUS server.

Provision Kerberos Server

Name	Description
DC Host Name (FQDN)	Enter your FQDN in the following format: machineName.domainName.com/net/.
DC Computer Domain	Specifies the domain name of the Kerberos server.
Keytab File	Type the encrypted Kerberos server key in this field.

Button	Description
Save	Saves your settings in the Authentication Servers page.
Cancel	Cancels your action and takes you to the previous page.

Active sessions

Viewing active sessions

Procedure

1. On the System Manager Web Console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **Active Sessions**.
3. On the Active Sessions page, the sessions are sorted in the **User ID** column.

Terminating Single Sign-On sessions

About this task

Use this functionality to terminate selected Single Sign-On (SSO) sessions.

Procedure

1. On the System Manager Web Console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **Active Sessions**.
3. On the Active Sessions page, select the check box beside the required sessions to terminate.
4. Click **Terminate**.

   The system deletes the selected sessions from the current sessions table. Administrators with terminated sessions are required to log on again.

Chapter 15: TLS support for Communication Manager notification

Overview of the CM notify sync feature

When you perform an administrative task from System Manager, the local database is immediately updated. If you execute the action through a Communication Manager SAT screen, or through a phone, or from any of the several management applications such as Site Administration, MultiSite Administration, Native Configuration Manager, or MyPhone, it is not immediately reflected in System Manager. This scenario creates an out-of-synch condition between the Communication Manager and System Manager.

The CM notify sync feature provides near-real time notifications from Communication Manager to System Manager whenever you execute certain tasks against a Communication Manager object from a system other than System Manager. The CM notify sync feature also provides notifications whenever the tti-m, tti-s, psa-u, psa-a, or psa-d logins perform their pre-defined actions against a Communication Manager station object.

After a Communication Manager sends notifications to System Manager, System Manager discovers the complete details of the task you preformed. The transmission of notifications in the form of event messages from Communication Manager to System Manager is based on the Communication Manager's existing rsyslog capability. The Communication Manager's rsyslog uses UDP or TCP to send event messages from the originating Communication Manager to the System Manager.

You can activate the CM notify sync feature from a new System Manager Web page. You can enable and disable the CM notify sync feature on a per Communication Manager basis. As a system administrator, you must specify the IPs of one or two System Managers to which the Communication Managers send event data using rsyslog. If your configuration includes two System Managers, the standby System Manager ignores the syslog messages until it becomes active.

Note:

The existing nightly default synchronization and any other scheduled synchronization operations are unaffected by the CM notify sync feature.

You need Communication Manager with 6.2 or above for the CM notify sync feature to work. Currently this is a one-way TLS.

The following tasks help you to configure TLS support in Communication Manager for the notify sync feature to work in System Manager. You must download the System Manager certificate and add the certificate in the Communication Manager Trust Store.

Downloading the System Manager certificate

Procedure

1. On the System Manager Web Console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. On the CA Functions page, click **Download pem file**.
4. After you download the .pem file, save the file to your system.

Downloading the pem file to Communication Manager

Procedure

1. Login to a Communication Manager Web console.
2. Click **Administrator** > **Server (Maintenance)**.
3. In the left navigation pane, click **Miscellaneous** > **Download Files**.
4. Select the **Files to download from the machine I'm using to connect to the server** option.
5. Click **Choose File** to browse to the downloaded certificate.
6. Click **Download**.

   The system displays the Download Files Results page with a message that the download is successful.

Adding a trusted certificate to Communication Manager

Procedure

1. Login to a Communication Manager Web console.
2. Click **Administration** > **Server (Maintenance)**
3. Click **Security** > **Trusted Certificates**.
4. Click **Add**.
5. On the Trusted Certificate – Add page enter the file name for the certificate you want to add. The certificate must be a .pem file. The name of the certificate must be the same as the one used in the ***Downloading the pem file to Communication Manager*** section.
6. To validate the certificate, click **Open**.

   After a successful validation, the Trusted Certificates – Add page displays the **issued-to**, **issued by**, and **expiration date** information for the certificate you are adding.

   Note:

   The system displays an error message if the certificate is not a valid certificate.
7. Select the **Communication Manager**, **Remote Logging** repositories from the list of trusted repositories.
8. Click **Add**.

   The system verifies the following:

   - The certificate name has a .crt extension. If the certificate name has a different extension, the system deletes it and replaces it with a .crt extension.
   - The certificate name is unique and does not already exist.
   - The certificate is not a duplicate certificate with a new name.
9. After adding the trusted certificate on the Communication Manager, connect to the Communication Manager command line as sroot through SSH.
10. Run the **`service rsyslog restart`** command to restart the syslog service.

Chapter 16: Changing the IP address and FQDN in System Manager

Prerequisite for changing the IP address and FQDN in System Manager

Before you begin

- Install System Manager on a system.
- Log on to the System Manager Web Console as admin.

Perform the following procedure to verify that all the extension packs are successfully deployed.

Procedure

1. On the System Manager Web Console, click **Services** > **Configurations**.
2. Click **Extension Packs**.
3. In the **Extension pack data** section, verify that the status of all the extension pack data is `success (confirmed)`.

   Create a backup using the **Services** > **Backup and Restore** service in the System Manager. Ensure that you backup the data successfully. Copy the backup data to a remote computer or to an external storage device, such as a tape drive or a DVD.

Related topics:

Changing the IP address and FQDN in System Manager on page 984

Changing the IP address and FQDN in System Manager

About this task

After you install System Manager, you can change the IP address, hostname, or the general network settings of the machine running System Manager from the System Platform Web Console.

Procedure

1. To log on to the System Platform Web Console, open your Web browser and type `https://<C-dom IP Address>/webconsole`.
2. Log in as administrator.
3. Click **Server Management** > **Network Configuration**.
4. In the **General Network Settings** section, change the values in the **Default Gateway**, **Primary DNS**, and the **Secondary DNS** fields.
5. In the **Domain Network Interface** section, for Bridge `avpublic,` change the netmask.
6. In the **Template Network Configuration** section, modify the following fields with the new values:
   - Change the IP address to System Manager IP address.
   - Change the FQDN to the new System Manager FQDN.
7. Click **Save**.
   The system displays the following confirmation message: `Changing network setting may require you to log in again into webconsole. Are you sure?`
8. After you confirm, the system displays the message: `Processing your request, please wait`.... After the processing and the network changes are complete, the system displays the following status message: `Settings updated successfully`.

   Note:

   Ensure that the new IP address or the host name is not already in use.

   After you click **Save**, the changes take effect on System Manager in about 30 minutes. This is not applicable if you modify only the General Network Parameters.

   If you modify the host name:

- The user interface password for System Manager automatically resets to the default password, admin123.
- All the UCM data is lost. You must enter the data again.

When the IP-FQDN script runs on the System Manager virtual machine, the system creates a log directory in the `/var/log/Avaya` location.

9. If the SAL Gateway is configured to receive SNMP traps from System Manager, click **Server Management** from the System Platform Web Console.
10. Click **SAL Gateway Management**.
11. Click **Launch SAL Gateway Management**.
12. Log in to System Platform as `admin`.
13. Click **Managed Element**.
14. If the FQDN has changed from the list, click on the entry with System Manager FQDN or old FQDN .
    The system displays the Managed Element Configuration page.
15. To modify the IP address, or FQDN, or both to the new IP address and FQDN, click **Edit**.

Related topics:

Prerequisite for changing the IP address and FQDN in System Manager on page 983

Changing the System Manager IP address and FQDN in the managed elements

For information on changing the System Manager IP address and FQDN in the managed elements, see the product documentation of the respective managed element.

Changing the IP address and FQDN of managed elements

For information on changing the IP address and FQDN of the managed elements, see the product documentation of the respective managed element.

Changing IP address and FQDN of managed element in System Manager

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select the registered element from the table.
4. Click **Edit**.
5. Update the value for the **Node** field in the Application section, and the **Host** field in the Access Point section.

Chapter 17: Troubleshooting System Manager

Overview

The section provides detailed information to help you resolve issues with Avaya Aura® System Manager. The troubleshooting section is intended for those who use System Manager to maintain, manage, and service Avaya applications and systems.

Some of the Avaya adopting products that System Manager currently supports:

- Avaya Aura® Session Manager
- Avaya Aura® Presence Services
- Avaya Aura® Communication Manager
- Avaya B5800 Branch Gateway
- Avaya Aura® Call Center Elite
- Avaya Aura® Contact Center
- CS 1000

Launching errors

System Manager Web console fails to open

Symptoms that identify the issue	System Manager Web console fails to open and does not display any error.
Cause of the issue	If you log in to the System Manager from the Web console when the CND service is not running, the log-in page fails to open and displays an error message.

Proposed solution

Procedure

1. To start the CND service, enter `service cnd start`.
2. To start the jboss service, enter `service jboss start`.

Tip:

If you run the **`init 6`** command, the system starts all services including CND.

Alarm errors

Alarms fail to reach ADC through SAL Gateway

Symptoms that identify the issue	Alarms fail to reach ADC through SAL Gateway. However, events log in System Manager displays the generation of alarms.
Cause of the issue	When you configure System Manager as Managed Element for SAL Gateway, the system displays the following error message: `Latest SAL model for System Manager is not pushed on this System Platform box, current model shows as SystemMgr_2.0.0.1 As a result, you fail to enable the Alarm option.`

Related topics:

Proposed solution on page 988

Proposed solution

Procedure

1. Through the command prompt interface (CLI), log on to the Console Domain (C-dom) of System Platform.
2. At the command prompt, enter the following commands:
   - `cd /opt/avaya/SAL/gateway/upgradeScripts`

- `/upgradeSALModels.sh`

The system populates the latest models. SAL Gateway automatically reflects the Solution Element Identifiers (SEID) attached to the latest model.

3. Configure System Manager as managed element for SAL Gateway. Alarms start flowing to ADC from System Manager.

System Manager generates hundreds of alarms

Symptoms that identify the issue

The sys_ConfRefreshConfig job fails with the following errors in the jboss server.log:

- A scheduled job failed to execute. Please see logs for more details.
- Illegal Argument Exception: Lookup is incorrect. Reason : javax.naming.NameNotFoundException: conferencing-ear-6.0.0.0.267 not bound

Cause of the issue

.

- Mismatch of version in the conferencing-ear file
- If any SSL negotiation error occurs, the system logs any further database queries in the postgres log files that causes the current issue.
- If the system is a 6.0.x upgraded setup, mismatch of JNDI name between the scheduler and Conferencing.

Related topics:

Proposed Solution on page 989

Proposed Solution

If you do not have the Conferencing solution deployed in your environment, disable the job to stop the logs or alarms.

About this task

Use this procedure to disable a scheduled job:

Procedure

1. Log on to the System Manager Web Console as a user that has privileges to make changes on the Scheduler Web page. For example, *admin*.
2. Click **Monitoring** > **Scheduler**.
3. Click **Pending Jobs** and look for *sys_ConfRefreshConfig*.

The system schedules the *sys_ConfRefreshConfig* job to run once per minute. If you do not find this job in the list of pending jobs, it means the job is disabled.

4. Check the status of the *sys_ConfRefreshConfig* job in the **Job Status** column. If the status is enabled, select the job and click **More Actions** > **Disable**.
   The system disables the *sys_ConfRefreshConfig* job.
5. If you do not find the job on the Pending jobs page, click **Completed jobs** and search for the job. Verify if the job is in disabled state. If the job is still in enabled state, repeat Step 4.

   You must disable any on-demand jobs created for sys_ConfRefreshConfig from both the pending jobs and the completed jobs list.
6. If the system does not open the Completed jobs page due to the stale entries:
   a. To delete the entries, enter the following command on the avmgmt database:

      ```
      DELETE FROM Sched_Job_Status jobStatus WHERE
      jobStatus.status_Id NOT IN( SELECT status.status_Id FROM
      Sched_Jobs jobs , Sched_Job_Status status WHERE
      jobs.job_Id = status.job_Id AND status.end_Time_Stamp =
      (SELECT MAX(st.end_Time_Stamp) FROM Sched_Job_Status st
      WHERE st.exit_Status NOT IN (0,1) AND jobs.job_Id =
      st.job_Id GROUP BY st.job_Id )) AND jobStatus.exit_Status
      NOT IN (0,1)
      ```

   b. To verify the number of times the job gets executed, run the following query:

      ```
      SELECT count(*) from sched_job_status;
      ```

      Verify that the value of the count is less. The completed jobs displays the list of all jobs that includes *ConfRefreshConfig*. If the ConfRefreshConfig job is in disabled state, enable the job and allow the job to run twice.

      The system stops the generation of alarms related to ConfRefreshConfig.

Related topics:

System Manager generates hundreds of alarms on page 989

System Platform errors

System Platform fails to detect the short hostname prior to template install

Symptoms that identify the issue

After the installation of the System Manager template from the System Platform Web Console, the template installation rolls back.

Cause of the issue

In System Manager 6.1, you must enter only the FQDN as the hostname. However, you can still enter the short name in the hostname field. After you install the System Manager template using the System Platform Web Console, System Manager runs a post install script for validation. The script delays by 30 minutes or fails to recognize the shortname for the **Hostname** field. As a result, the template installation rolls back.

Related topics:

Proposed Solution on page 991

Proposed Solution

Procedure

1. Open the `SystemManager.ovf` file from the build location.
2. To detect the short hostnames prior to the System Manager template installation, add an XML attribute to the OVF templates in System Platform for template fields similar to the following:

```
<ovf:Property ovf:key="smgr.hostname" ovf:type="string"
ovf:qualifiers="MinLen(1)"
                                ovf:def-value="" ovf:userConfigurable="true"
ovf:requirefqdn="true" or ovf:requireip="true" or generic
attribute=”----” >
<ovf:Description>Hostname: System Manager FQDN</ovf:Description>
</ovf:Property>
```

   System Platform detects the use of shortnames in the fields before the System Manager post install script validates.

3. In the `SystemManager.ovf` file, change the checksum, sha1sum and update the `sha1sum_report.txt` file in the build location.

System Manager captures the new parameters and uses them in the post install script for validation.

Certification errors

System Manager does not support third-party certificates

Symptoms that identify the issue System Manager does not support third-party trust certificates.

Related topics:

Proposed solution on page 992

Proposed solution

Before you begin

- Obtain the certificate that has the System Manager hostname as CN, and signed by the third-party Certificate Authority (CA).
- If required, store the third-party certificate and subordinate CA certificates in a PKCS#12 container with the corresponding private key.

About this task

To install and use the third-party certificate for System Manager Web interface, perform the following high level steps:

Procedure

1. Replace the System Manager Web server certificate with a third-party certificate.
2. Update the trust stores for internal services, clients, or managed elements with third-party root and subordinate CA certificate.

   For more information, see *Application notes for supporting third-party certificate in Avaya Aura® System Manager 6.1* on the Avaya Support Site at http://support.avaya.com.

Bulk import and export errors

Import utility fails to import the users of specific time zone

Symptoms that identify the issue	Using the import utility, when you import the users with the (+01:00) Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels, Sarajevo time zone, the system fails to import the user data.
Cause of the issue	Bulk import feature does not take the timezone string that the User Management page displays. Also, the bulk import feature expects the timezone offset information to be present for the timezone attribute in import XML file.

Related topics:

Proposed solution on page 993

Proposed solution

The system does not display the timezone information of the user that you import on the User View profile page. Therefore, for each imported user, you must manually update the timezone information.

Before you begin

- Log on to the System Manager Web Console.
- Import the user data.

  To import the user data, click **Users** > **User Management** > **Manage Users** and click **More Actions** > **Import Users**.

Procedure

To successfully import the users, perform one of the following procedures:

- Click **Users** > **User Management** > **Manage Users** and perform the following:
  i. Select the user and click **View**.
  ii. On the User Profile View page, ensure that the timezone offset information in the **Time Zone** field. For example, (+01:00) Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels, Sarajevo.

- For each user, in the import XML file, remove the timeZone attribute tag. For example, remove:

```
<timeZone>(+01:00) Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels,
Sarajevo</timeZone>
```

Miscellaneous errors

Authentication of the LDAP user to System Manager fails

Symptoms that identify the issue	Authentication of the LDAP user to System Manager fails.
Cause of the issue	The customer LDAP has login names with DN in the format, `cn=<loginname>,oc=<oc-value>,dc=<dc-value>,dc=<dc-value>`. The login name does not have the domain information.

Related topics:

Proposed solution on page 994

Proposed solution

Using the Subject Mapping table, you can map an LDAP user to a System Manager user. Therefore, System Manager authenticates the LDAP username without @domain and then maps to the correct user in System Manager.

Before you begin

- Obtain the System Manager login name and the corresponding identities.
- Log on to System Manager.

Procedure

1. To map the users in the User Management and the LDAP, enter the user name in the **CSSecurityIdentity** table.
2. To populate the **CSSecurityIdentity** table, use the bulk import functionality as shown in the sample XML file.

```
<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList xmlns:delta="http://xml.avaya.com/schema/
deltaImport" xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
  <delta:userDelta>
    <loginName>janedoe@avaya.com</loginName>
    <securityIdentity>
      <identity>janedoe</identity>
      <realm>admin</realm>
      <type>principalname</type>
    </securityIdentity>
  </delta:userDelta>
</delta:deltaUserList>
```

Element Manager errors

Removed Communication Manager reappears on the System Manager Web Console

Symptoms that identify the issue

Communication Manager that was removed earlier, reappears on the System Manager Web Console.

Cause of the issue

In System Manager, the problem occurs when:

a. Two Communication Manager systems with the same name exists.

b. Out of the two Communication Manager systems, you manually add one system and the other system gets added from **Elements** > **Inventory** > **Inventory Management** > **Discovery**.

c. You remove the two Communication Manager systems.

The system removes the entry of Communication Manager from **Elements** > **Inventory** > **Manage Elements**. However, System Manager still displays the two Communication Manager voice systems on the **Elements** > **Inventory** > **Synchronization** > **Communication System** page.

Related topics:

Proposed Solution on page 995

Proposed Solution

Assume the IPTCM database has two entries of Communication Manager systems with rtsappids 50 and 100. Use this procedure to remove the Communication Manager system with

the rtsappid 100 and reinstate the entry of the legitimate Communication Manager with rtsappid 50.

Procedure

1. To set the rtsappid to null and the name to any arbitrary value for Communication Manager that has rtsappid 100, run the following query:
   ```
   update ipt_cm set cmname='ABC',rtsappid= null where id = 100;
   ```
2. To modify the IP addresses in the **ipt_cm_conn** table, run the following query:
   ```
   update ipt_cm_conn set ipaddress1='1.1.1.1' , ipaddress2='1.1.1.1' where
   id = 100;
   ```
3. To run the maintenance job for Communication Manager, on the System Manager Web Console, click **Services** > **Scheduler** > **Pending Jobs**.

   The system removes the entry cm_id=100 from the tables **ipt_cm** and **ipt_cm_conn**.
4. To add the entry of the Communication Manager system again, from Runtime Topology System (RTS), provide the IP address and the name of the legitimate Communication Manager system.

   Note:

   If the details you enter does not match with the legitimate Communication Manager, the system adds a new entry for the Communication Manager in the **ipt_cm** table.
5. To retrieve the ID of Communication Manager that you entered in step 4, from the **rts_applicationsystem** table, run the following query:
   ```
   select id,name from rts_applicationsystem;
   ```

   The Communication Manager ID is the rtsappid for the **ipt_cm** table.
6. To update the rtsappid in the **ipt_cm** table with the ID you retrieved from the previous step, run the following query:
   ```
   update ipt_cm set rtsappid=? where id = 50;
   ```

   Verify if the synchronization is working for Communication Manager.

   The system modifies the rtsappid for Communication Manager.

Deletion of Communication Manager from RTS fails

Symptoms that identify the issue	Deletion of Communication Manager from Runtime Topology System (RTS) fails if the Communication Manager system is part of an Uniform Dialing Plan (UDP) Group.

Cause of the issue When you attempt to delete Communication Manager from RTS, the system checks for the resource name UDP Group instead of UDP_Group. If the system fails to find UDP_Group, Communication Manager does not get deleted from RTS.

Related topics:

Proposed solution on page 997

Proposed solution

Procedure

1. On the System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. To delete Communication Manager from RTS that is part of a UDP group:
   a. Select the check box for the Communication Manager system that has the **Type** field set to `UDP_Group`.
      You set the **Type** field to `UDP_Group` from **Users** > **Groups & Roles** on the Group management page.
   b. Click **Delete**.

Note:

Do not search for the GLS Group **UDP Group**.

Appendix A: Firewall implementation in System Manager

Firewall basics

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources. The firewall controls what outside resources its own users can have access to. Simply put, a firewall is a program or a hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters it is not allowed through.

Firewalls use one or more of three methods to control traffic flowing in and out of the network:

- Packet filtering - Packets or small chunks of data are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.
- Proxy service - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.
- Stateful inspection - A newer method that does not examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match the information is allowed through. Else, it is discarded.

Firewall implementation in System Manager

The System Manager firewall implementation uses packet filtering and stateful inspection techniques.

Salient features of the firewall

- Supports unlimited access to loop back address through packet filtering.
- Drops all inbound packets by default, allows all outbound packets, and allows all packets that are to be forwarded through packet filtering.
- For TCP packets, the firewall checks for various combinations of the TCP flags to ascertain whether a packet is valid or not. There are a set of standard rules for identifying valid TCP packets, and these have been incorporated into the System Manager firewall.
- Supports stateful inspection of packets. The firewall checks the state of all inbound and outbound packets for secure communication. For inbound packets the state must be either Established or Related. For outbound packets the state must be either New, Established or Related.
- Disables ICMP timestamp responses as this allows an attacker to know the date which is set on your machine. This defeats all the time based authentication protocols.
- Allows inbound communication on ports that are reflected as a part of the System Manager 6.2 port matrix document.

Configuring the firewall in System Manager

About this task

The firewall rules are captured in the file `$MGMT_HOME/utils/bin/firewall/ConfigureIptables.sh`.

Procedure

To configure and enable the firewall, execute the command `sh $MGMT_HOME/utils/bin/firewall/ConfigureIptables.sh`.

Enabling and disabling the firewall

Procedure

1. To query the status of the firewall, execute the command **`service iptables status`**.
2. To enable the firewall, execute the command **`service iptables start`**.

3. To disable the firewall, execute the command **`service iptables stop`** .

Modifying the System Manager firewall rules

Procedure

1. To modify the System Manager firewall rules, edit the `$MGMT_HOME/utils/bin/firewall/ConfigureIptables.sh` file.
2. Append the rule at the appropriate position in the firewall chain.

   Note:

   The firewall rules are applied on a packet in top-down fashion. Ensure that the additional rules appear at the appropriate position in the firewall rule chain.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X