Network Security Analyzer

User Guide

April 2013 Edition

Corero Network Security
1 Cabot Road
Hudson, MA 01749
U.S.A
www.Corero.com

Copyright and Trademarks

Table of Contents

Chapter 1: About This Guide

This guide explains how to use the installed Corero Network Security Analyzer (NSA) platform, including the Central Server, Data Collector and Regional Server.

Audience

The reader should have system administrator experience with networking and information security technologies, be comfortable using software on distributed enterprise servers, understand TCP/IP networking and remote logging, and understand network protocols and standards.

Related Documentation

You can download the following related documentation from the Corero Support Center at http://www.Corero.com/support

Conventions

Text formatting in this guide uses the following conventions:

IMPORTANT: identifies important information impacting system operation or information security.

NOTE: identifies information that should be considered.

TIP: identifies information helpful to performing a procedure or solving a problem.

Technical Support

Contact support@Corero.com for all trial and purchased product support.

For warranty, maintenance, and license information, visit www.corero.com\agreements.jsp.

Chapter 2: Introduction

As IT becomes the nerve center of today's wired enterprise, organizations are under increasing pressure to implement best practices to control growing security, risk and compliance challenges such as internal and external threats, operational issues, intellectual property protection, privacy and regulatory mandates. Despite network and security operation centers and operational risk management groups emerging to help remedy the situation, when faced with the challenge of building out a unified IT risk management framework, they discover no integrated security, risk and compliance solutions currently exist. As such, numerous point solutions from multiple vendors are cobbled together, resulting in disparate silos of data that are costly and complex to manage. The need to manually connect the dots to discover the root cause of a problem proves timely and requires excessive resources.

Corero Network Security Analyzer, an integrated security and compliance management framework improves IT security and increases operational efficiency while reducing total cost of ownership. Using a patent-pending and highly scalable data model, Corero's security management platform integrates Security Information and Event Management (SIEM) data into a single unified system. With end-to-end root cause analysis and a robust correlation engine, NSA provides visibility across network, server and application layers to enable organizations to gain a comprehensive understanding of the infrastructure's overall security.

Corero Network Security Analyzer 5.1 helps you:

- Gain end-to-end visibility into the infrastructure
- Deliver cross functional cooperation between network security and compliance teams
- Increase operational efficiency and productivity
- Minimize time to identify and fix security incidents
- Meet compliance mandates across numerous regulations
- (e.g., FISMA, GLBA, HIPAA, PCI and SOX)
- Implement security best practices and processes
- (e.g., CobIT, ISO 17799 and ITIL)
- Streamline resource requirements and reduce overall costs
- Improve business accountability and measure ROI

Components in Corero Network Security Analyzer

NSA consists of two main components:

- Corero Network Security Analyzer Server
- Data Collector

NSA Server: All the network devices to be analyzed are added, profiles and alerts are configured so that when Data Collector fetches the event logs in a live environment, it can report on the event logs. These reports help the security administrator to take corrective actions and safeguard networks.

Data Collector: Collects event logs automatically from all the configured network devices, compresses them into delta files and sends it across to the NSA Server for generating reports.

Chapter 3: Getting Started

This chapter provides instructions how to start, configure default options, and create profiles using NSA 5.1.

Starting NSA

This section explains how to start NSA (registered version or a trial version).

Once the software has been successfully installed NSA can be started by double clicking on the NSA icon created on the desktop.

Corero Network Security Analyzer Desktop Icon

Alternatively, you can start NSA by typing the installed Web site URL in the address bar of the browser window.

Provide the default user credentials created during the NSA installation on the login screen. The first time you start your NSA software, you are asked to obtain a trial/permanent license key by providing the auto-exported CoreroNSASystemIdentifier.txt file. During the evaluation period, NSA is as competent as the purchased product. At the end of the evaluation period, the evaluation license expires, thereby ceasing the NSA operations.

To ensure uninterrupted Security Information and Event analysis and to protect your network, you should purchase the product at the earliest.

Navigating through NSA

By default NSA starts opens with the **Dashboard** console. From this screen you can navigate to Setup options, Manage nodes, Monitoring and Reporting portals and all of the features provided in NSA.

Help

Extensive online help is available for all the modules by clicking  the top right-hand corner of each screen. If you have any questions about NSA, our support team will be glad to assist you.

An Important Note on File Names in This Book

Substitute the name “Corero” any place in this guide where you see a file name or path name that includes the name “Top Layer” or the initials “TLN.”

Chapter 4: Data Collector

The NSA Data Collector helps you do away with manual configuration of devices. While some devices can export log files in a readable format, others typically do not write log information to a readable file. In such cases, NSA relies on a Data Collector to capture log information. The NSA Data Collector helps eliminate the need for manual configuration of devices. It automatically detects new device IP's in the log data, which are subsequently displayed from the Devices tab of Central as unconfigured devices.

The Data Collector can be installed on any machine in the network. One of the first things you should do after installing NSA is to configure a Data Collector. While doing this, you can also backup all the logs that are streamed to the Data Collector from various devices by configuring a backup Data Collector.

NOTE: The backup Data Collector can be a non-NSA or NSA Data Collector. The NSA Data Collector forwards all the packets that it receives from the configured devices to the backup Data Collector. Please note that a backup Data Collector cannot forward any data to the NSA Data Collector and in case that happens, the NSA Data Collector drops all such data packets.

When you create a profile, you can choose to collect your log files from:

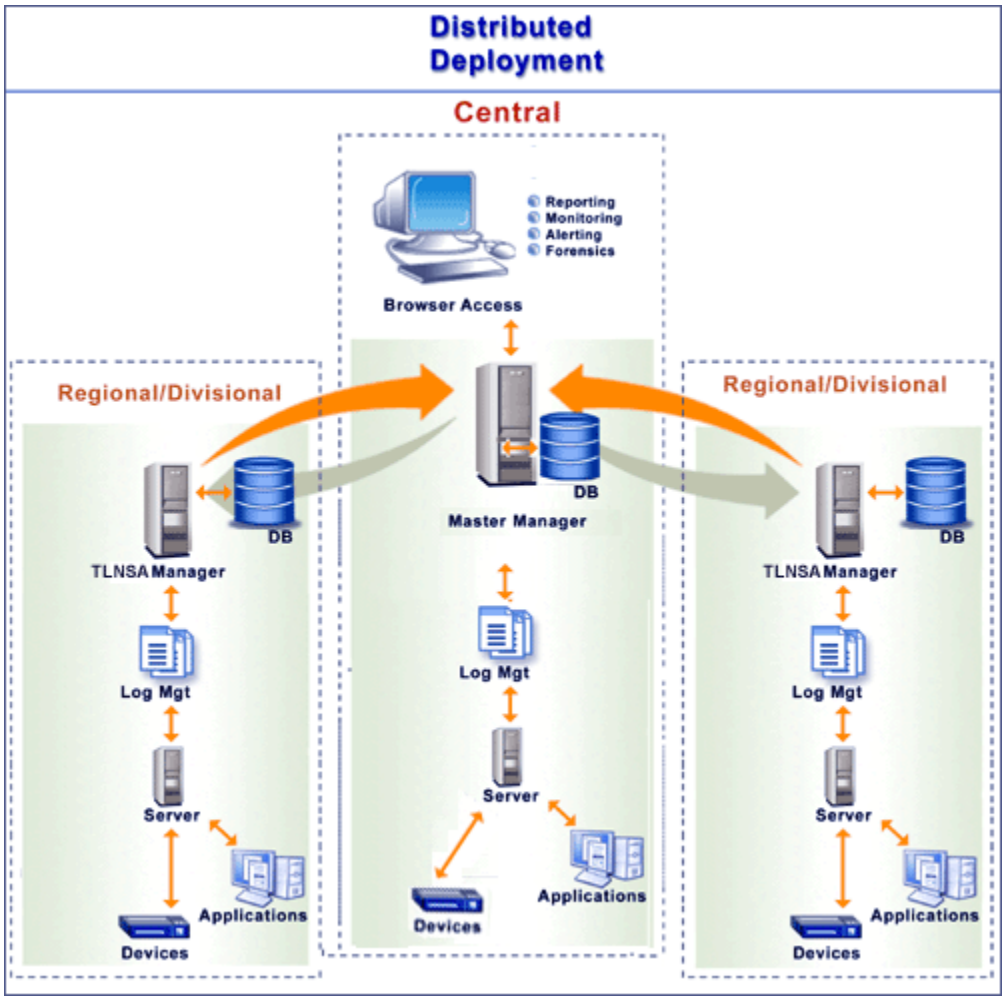
- Integrated Database
- File

Integrated Database: The NSA Data Collector streams log file data to the data collector service installed on the NSA machine, where it is parsed and stored in the database.

Once the data collector is configured, it automatically updates the delta file to the database on a regular basis without intervention from the administrator.

File: Use this option to report on static log files obtained from a manually added device (device that is not configured to send data to the Data Collector).

Deployment Schema



NOTE: Since NSA Data Collector runs as a Windows service, it must be installed only on Windows server 2003 machine.

TIP: To configure NSA Data Collector, you must have administrator privileges.

Windows XP with SP2 has strict Windows Firewall rules, so it blocks all external applications. Please configure your Windows Firewall to unblock the following:

a. Allow remote administration from the Group Policy Settings for NSA Apache Server.
b. Provide exception for Data Collector, NSA Apache Server, and other related executable files.
c. Provide exception for the NSA ports.

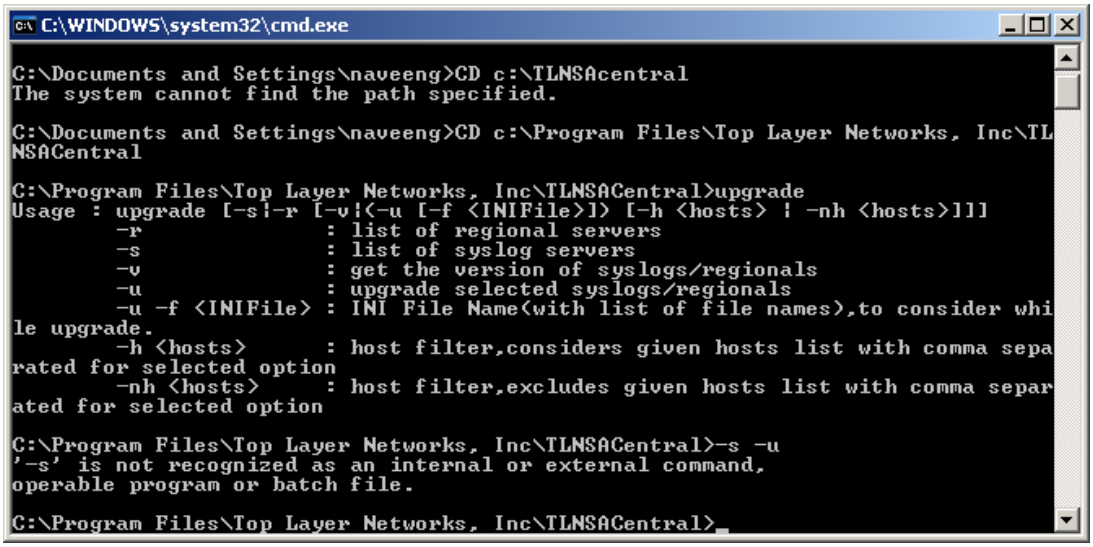
Upgrading Remote Data Collector(s)

During the upgrade you are prompted to upgrade the following components.

- NSA Server
- Data Collector

To upgrade the Data Collectors associated with the NSA server, go to the <your path…\CoreroNSACentral> and run the upgrade command from the CLI. Using this tool, based on the requirement, you can upgrade all the associated Data Collectors or only the regional Data Collectors.

Upgrade - Data Collector



After the upgrade, all or selected Data Collectors will be upgraded to the latest version.

To upgrade the Data Collector installed on the local machine you can also use the following shortcut:

Start > Programs > Corero Network Security Analyzer v5.1 > Install Data Collector.

Important: NSA notifies the admin user of any failed upgrades through Admin Messages on the main screen. Admin user can acknowledge it and can retry to upgrade.

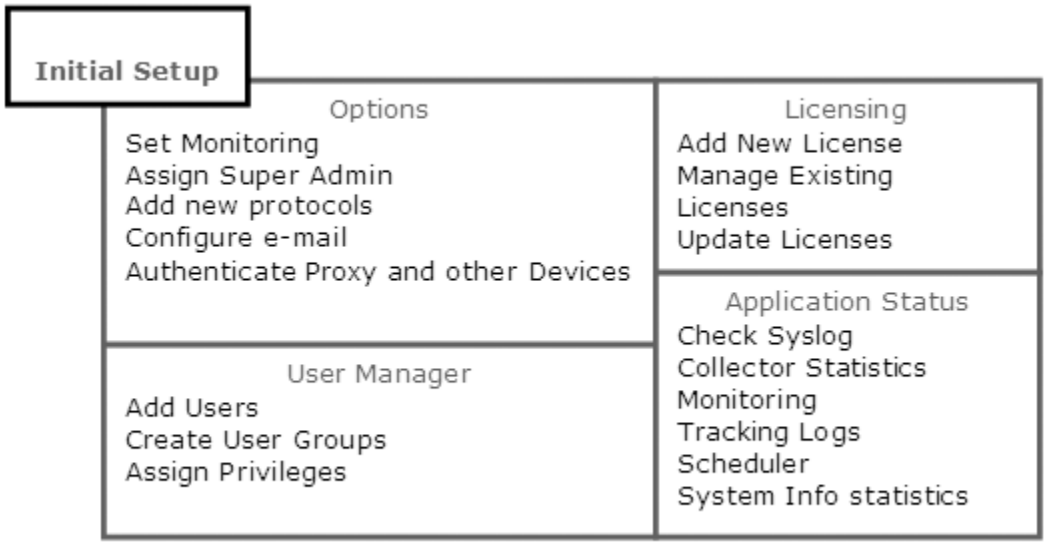
Chapter 5: Setup

NSA analyzes logs generated by your devices and provides an assessment of your enterprise network from outside in and inside out. Detailed picture of network activity is presented in the form of reports in HTML, MHTML, Word, Excel, PDF or Text formats.

Before you start exploring the reporting, alerting and monitoring capabilities of NSA, prepare the application by licensing the devices, creating users, assigning collection policies, configuring e-mail server and so on. The following sections explain each step in detail.

Setup - Options

- Licenses
- Options
- Reports Catalogue
- Status
- Users



Chapter 6: Licenses

This chapter provides information on how to license your copy of NSA and the devices you want to report on. It also explains how to manage your licenses.

License Requirements

At the time of first installation, NSA automatically creates a machine-specific trial license key using the MAC address. Once the license key is generated, you cannot use it to run NSA on any other machine. The trial license key can be used to license 10 devices. Each device can be analyzed for 21 days after it is licensed and the trial will expire 21 days after the last device is licensed. If the trial period has not been enough to evaluate the application, write to Corero requesting an extension. For a permanent license, use the Export Identifier to create a text file C:\Program Files\Corero\Corero Network Security Analyzer\CoreroNSA\CoreroNSASystemIdentifier.txt that stores the device identifier information. Send the file to Corero, and we will generate a license key for you.

If you have more than one device to license, let us know the number and we will generate an appropriate license key. Run the batch file from the CLI to add the license -

Usage from the CLI: AddLicense.bat <Absolute Path of the NSA License file>

Licensing Devices Identified by the Data Collector

When a new device ID streamed by the Data Collector is detected, it is added under the Data Collector as UnknownDeviceId. Click the UnknownDeviceId link and specify the criteria based on which you want this device licensed.
A device can be identified by any of the following identifiers:

- Internal IP
- External IP
- Device ID
- UId

Select an identifier and click **Save**. Later license the device/host from the license manager.

NOTE: Only licensed devices can be reported on.

Licensing a Configured Device

Follow the steps described below to license a Configured device:

1. Identify the IP address in the log file and add it in the **Devices/Groups**.

2. On the **License Manager** screen, select the **Licenses** tab.
3. Select a license key and click **Manage**.
4. Click **Add Device**. The **Add Device** screen opens. Select the device you want to license and click **Save**.

NOTE: The specified ID that is either internal/external IP or device ID must match the one provided by the device in the log files.

The License Manager Screen

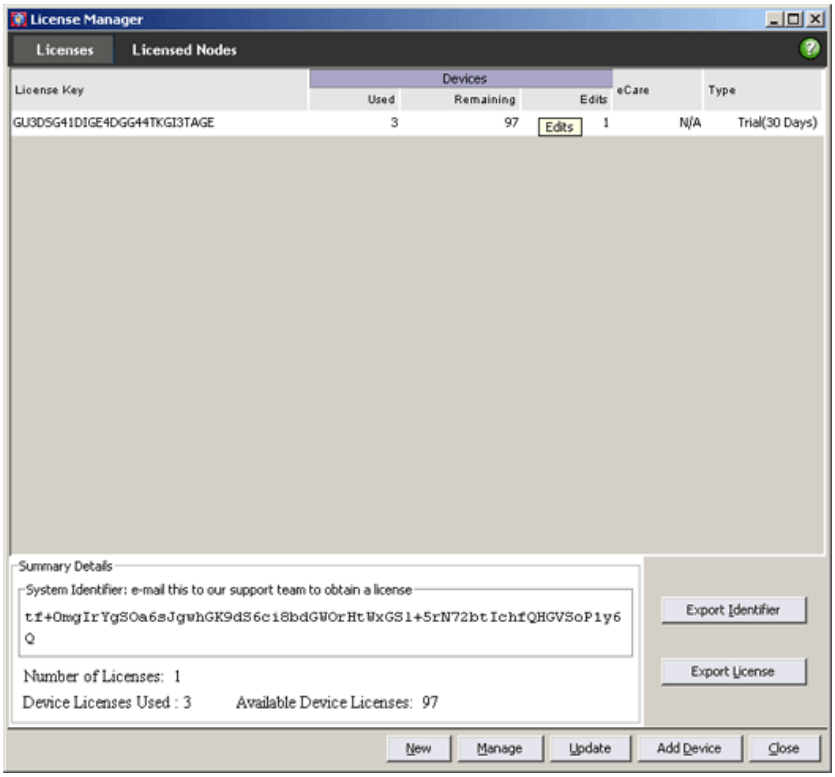
The License Manager comprises of Licenses and Licensed Devices tabs, each of which is explained in the sections below:

Licenses

On this screen, you can add, manage, update, or delete a license. It also displays the following information:

- License Key
- Devices – Used and Remaining licenses
- Type

Licenses Screen



Adding a License

You can add a new license on this screen. A license can be added in any of the two following ways:

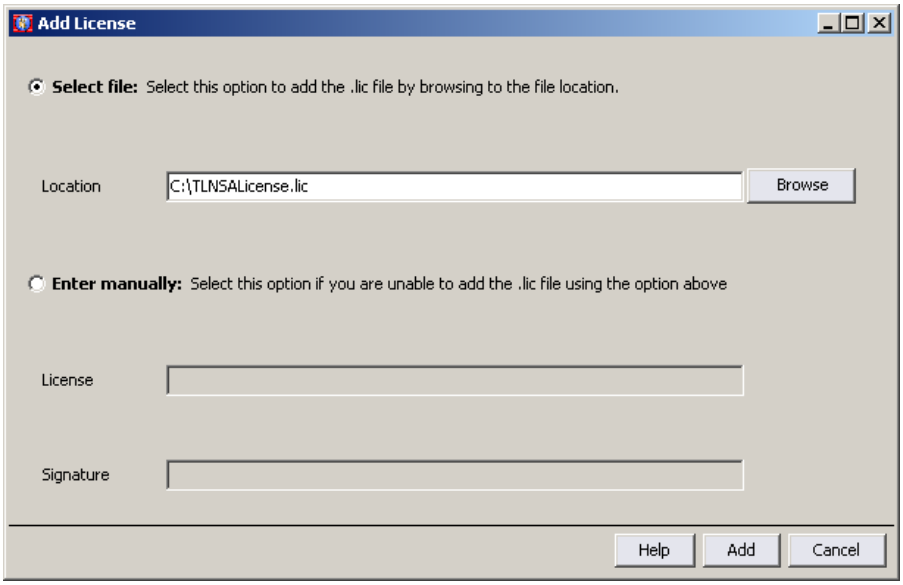
- Select file
- Enter Manually

Follow the steps described below to add a license:

1. Click **New**. The **Add License** screen appears.
2. If you have selected the Select file option, browse to the path where the .lic file is located.
3. If you have selected the Enter manually option, enter the license and the corresponding signature key in the text area.
4. Click **Add**.

NOTE: Before licensing a device, make sure it is configured.

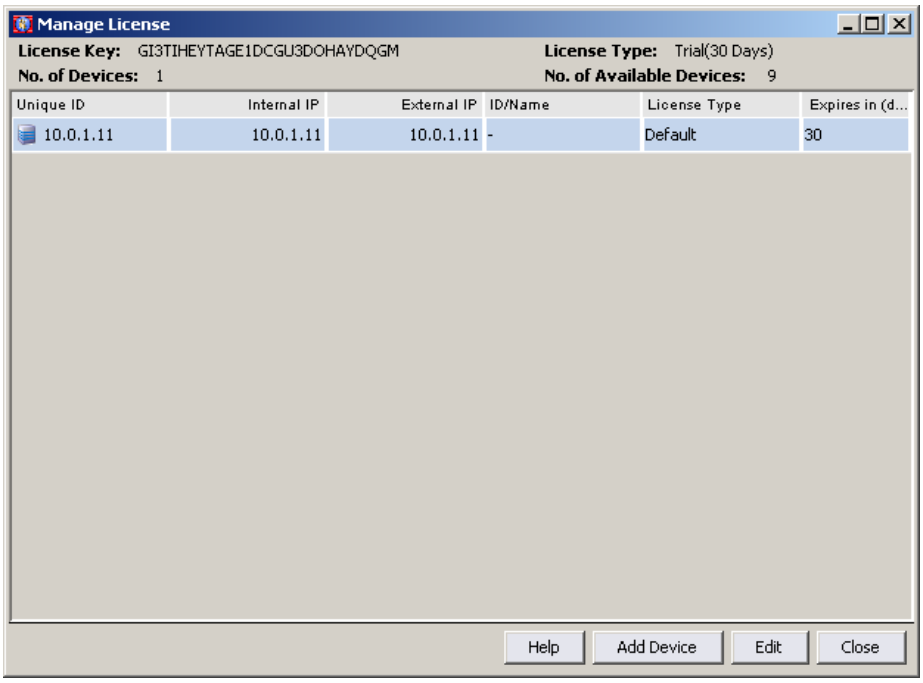
Add License Screen



Managing a License

You can manage an existing license key from here. You can also view the count of devices that have been licensed and also those yet to be licensed.

Manage License



NOTE: To manage license key, select the license key and click the **Manage** button available in the License Manager > Licenses tab.

Adding a Device

Follow the steps described below to add a device:

1. Click **Add Device**. The **Add Device** screen appears.
2. Select the device that you want to license from the list of unlicensed devices.
3. Click **Save**.

Editing a License

Device: You can replace an existing device with a new device. Before doing this, make sure that the device that you want in place of the existing device is added in the Devices/Groups and available in the License Manager as an unconfigured device.

Follow the steps described below to edit a device:

1. In the **Manage License** window, select a device and click **Edit**.
2. Enter the IP address of the device you want in place of the existing device.
3. Click **OK** to confirm.

NOTE: You can edit a primary device license not more than twice.

Updating a License

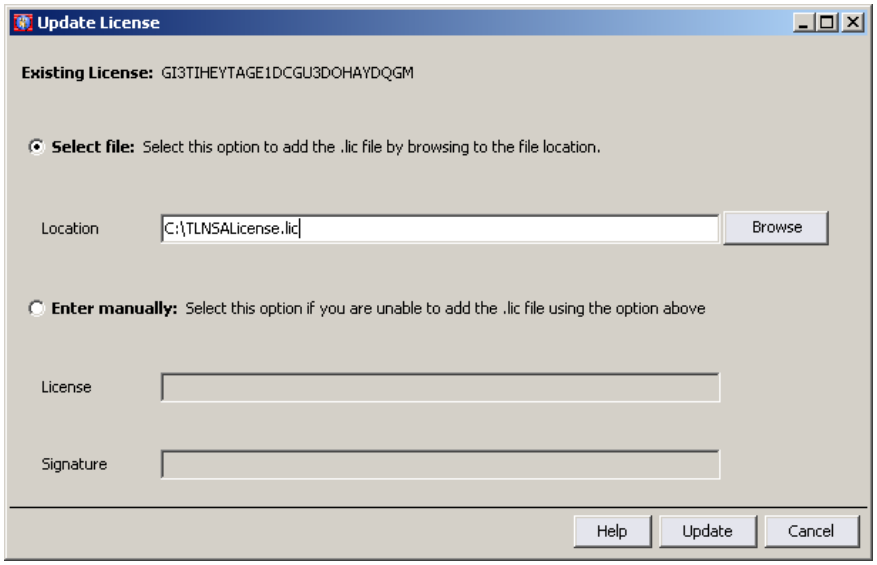
Use this feature when you need to:

- Increase the existing keys capability to license more number of devices.
- Extend the validity period of eCare associated with the selected license key.

You can update a license in two ways:

- Select file
- Enter manually

Update License



Follow the steps described below to update a license:

1. In the **License** tab, select a license and click **Update**.
2. If you have selected the **Select file** option, browse to the path where the .lic file is located.
3. If you have selected the **Enter manually** option, enter the license and the corresponding signature key in the text area.
4. Click **Update**.

Export Identifier

Click this button to save the Network Identifier to a text file. The Export Identifier file is located in the NSA installation directory. The identifier is exported to **<Your path>\CoreroNSACentral\CoreroNSASystemIdentifier.txt**. To generate the license key, you must export this file to Corero Network Security manually.

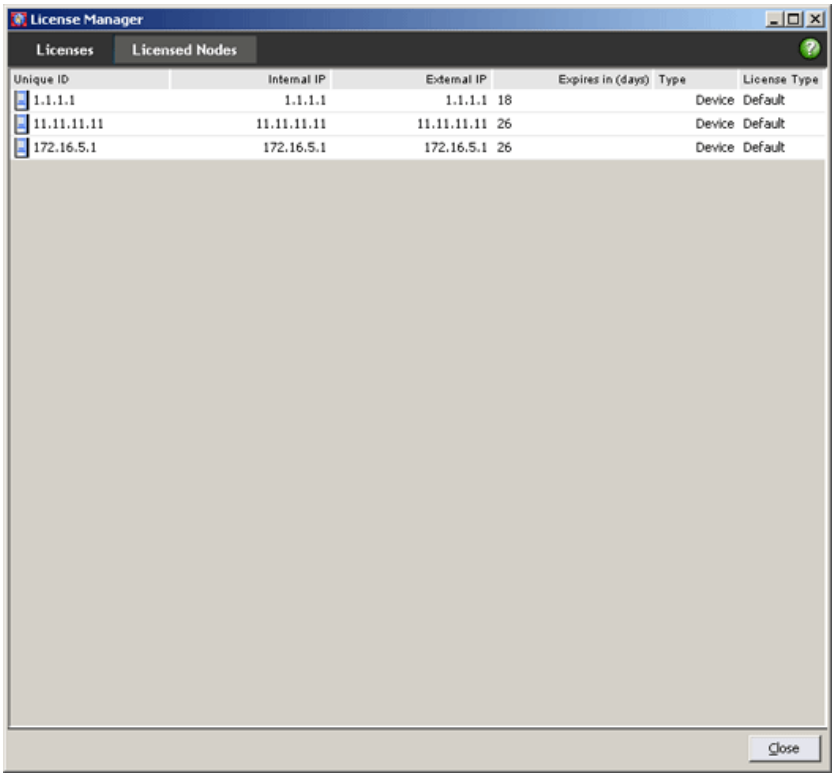
NOTE: Alternatively you can copy the System Identifier displayed in the Summary Details and mail it to Corero Network Security.

Export License

Use this option to keep a backup copy of your license. The exported .lic file can be used for communicating with Corero in case of requesting trial extensions or modifications. For additional information, please contact the reseller from whom you purchased the software, or contact our support team at support@Corero.com.

Licensed Nodes

This screen displays all the licensed nodes, type of license and number of days left for each license to expire. You can view the nodes based on Type of License or on the Type of Node (device) that is being licensed.



NOTE: Once a primary device is licensed, all virtual devices associated with it are automatically licensed.

Chapter 7: Options

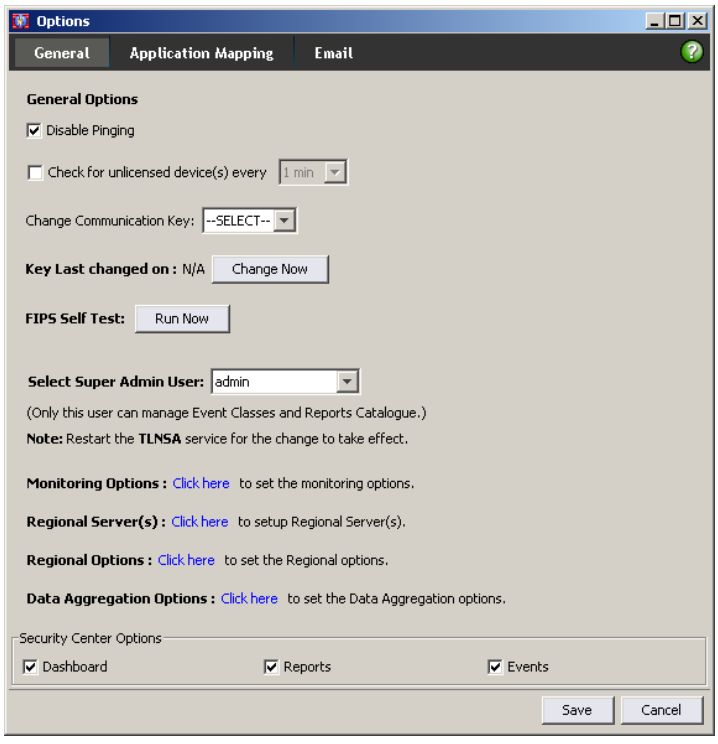
You can specify global settings to all the profiles created by the user and take control over the way NSA works.

- **General**: Use this to disable pinging, check for new devices identified by Data Collector, set Monitoring options, Add Regional Servers and specify the database and forensic delta upload frequency and also able to specify the data aggregation options on the central server.
- **Application Mapping**: This tab lists all the common protocols. All information in the log files pertaining to protocols will be analyzed based on the protocols displayed in the list. You may also add new protocols to the existing list.
- **E-mail**: Use this tab to specify default protocol your e-mail client uses and the user account you want NSA to use. These settings will be used to mail the generated reports.

NOTE: A Power User can only access the E-mail tab.

General Settings

The General Settings Tab



Disable Pinging: You can enable or disable pinging activity from the Data Collector which at times occurs frequently and hence makes the network busy. By disabling pinging, you can keep a check on the ping operation performed by the Data Collector to identify the status of devices configured to Data Collector.

Check for new devices every: Select this check box to check for the unconfigured devices every:

- 1 min
- 10 min
- 30 min
- 1 hour

Based on the interval selected, a pop-up window **Unlicensed Devices** is displayed whenever a new device is detected, you are prompted to configure and license it.

Change Communication Key

A Communication Key (AES Key) is derived from a New RSA Private Key and timestamp specifically for encryption of communication data. The Communication key can also be force-changed at any time from our GUI or can also be scheduled to be changed every week or month.

Select this check box so that you can schedule the change of Communication Key accordingly:

- None
- Weekly
- Monthly

To immediately change the communication key, you can use the **Change Now** option. You can also observe the details of last time when this key was changed.

NOTE: Using the Change Now option will restart the NSA mainengine.exe.

FIPS Self-test

Admin User (Crypto Officer Role) is the person with access privileges to install, configure and initialize the NSA cryptographic software.

A Crypto Officer can also request the module to perform self-tests using the FIPS Self-Test button provided in the **Setup** > **Options** window of the NSA GUI.

When this option is selected, NSA instantiates the FIPS test suite and performs the following group of self-tests. FIPS recommended cryptographic functionality will be available only when all the test suite requirements recommended by FIPS are successful.

- Continuous RNG test

- HMAC and SHA-1 test
- AES & RSA Encryption/Decryption test
- Pairwise_aes and pairwise_rsa tests
- Test Suite Zero-ization

NOTE: Federal Information Processing Standards specify the Security requirements for Cryptographic modules.

Selecting a Super Admin user

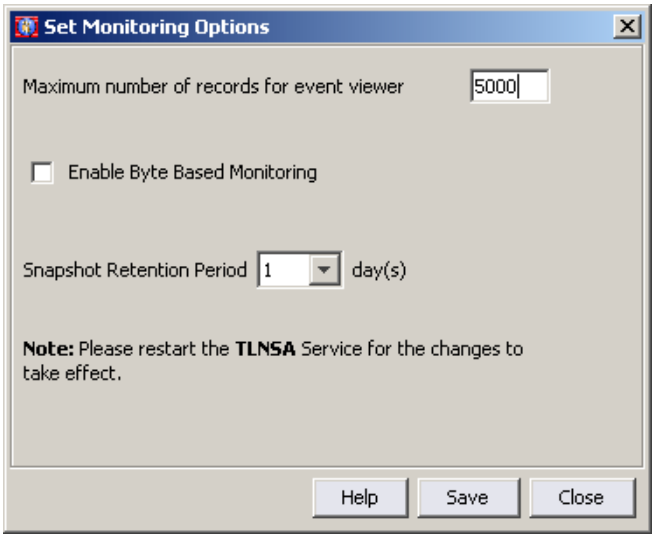
Select the super admin user from the drop-down list to assign the privilege to create/modify Event Classes, Reports Catalogue and also can change/reset the threat level associated with an event displayed in the event viewer, graph types and reports.

Selecting the admin user:

1. All the admin user accounts defined from the User manager are shown in the drop down list.
2. Select a user account that will be responsible for changing/resetting the threat levels, managing Event Classes and Reports Catalogue settings.
3. Restart the CoreroNSACentral Service for the changes to take effect.
   Note: If new users are added in the current login, use the Refresh button from the User Manager to re-populate the admin user drop-down list.

Monitoring Options

Click on the link **Click here** and the Set Monitoring Options window opens where you can set the monitoring options.



Maximum number of records for Event Viewer: Use this option to specify the maximum number of records that you want the event viewer to display.

NOTE: In a distributed setup, number of records displayed in the Central server is calculated on the basis of number of regional servers paired with the central i.e., [Default 5000 Events + (Number of Regional Servers*5000)]. For example if there are 3 Regional servers in the setup, total number of events displayed will be [5000+ (3*5000)] =20,000 events.

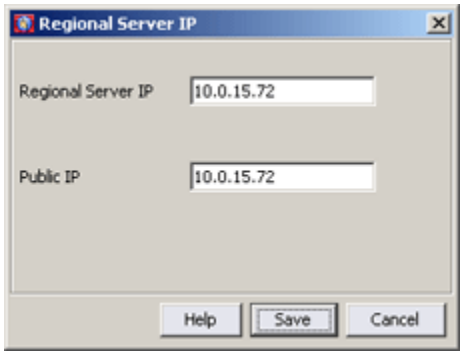
Enable Byte Based Monitoring: Enabling this option lets you view and monitor events by both Hits and Bytes.

Snapshot Retention Period: By default all monitors have the Snap utility using which NSA takes a snap of the monitor every one hour and maintains them for comparative analysis. You can specify the snapshot retention period ranging from 1 up to a maximum of 30 days.

NOTE: Restart the NSA server for the changes to take effect.

Manage Regional Server(s)

Regional Server informs Central server about its existence through its IP address. In a network, the device on which the regional server is installed could have multiple NIC cards, so there is a possibility that its IP address could differ. In order to resolve IP of such regional servers, provide the public IP address of the regional server. Central server would then detect the Regional Server using the public IP address.



Click on the link **Click here** and the Regional Server IPs window opens, where you can setup the regional servers.

Adding a Regional Server

Click on the Add button in the Regional Server IPs window and the Regional Server IP window opens where you can provide the IP address of the regional servers.

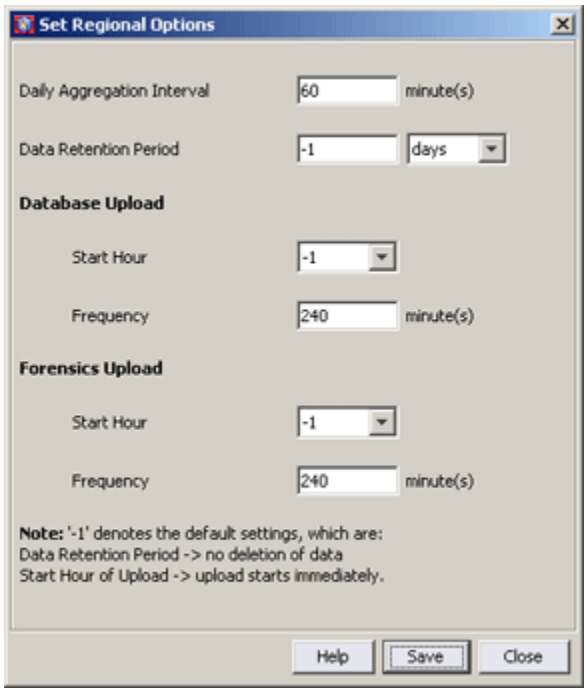
1. Provide the Regional Server IP and the public IP using which the Central server identifies the regional devices.
2. Click **Save**.

Set Regional Options

From the Central server, you can specify the time period for retention of data in the regional server and the daily aggregation time interval.

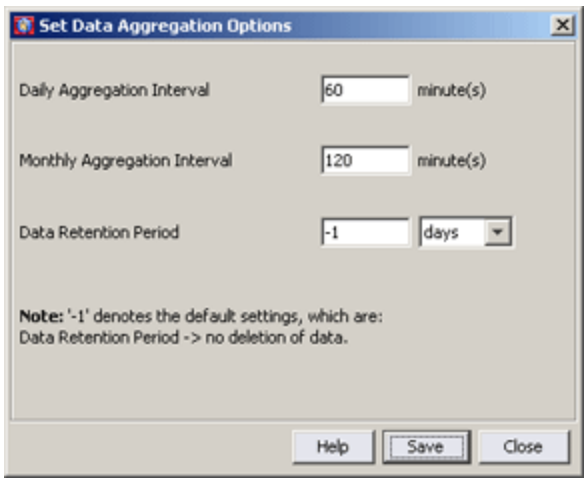
Regional server processes the log data as part of load balancing activity and uploads the central database with reporting deltas and forensic deltas. From the Set Regional Options window you can specify the start time, frequency at which the Database and Forensic deltas are uploaded to the central server for each day.

NOTE: By default all the data is retained in the database, Database and Forensics upload is performed immediately unless specified by the user.



Set Database Options

Using the Data Aggregation Options provided in the General options window, you can specify the Daily Aggregation Interval and Monthly Aggregation Interval and Data Retention period for the data in the Central server. These options are helpful to effectively manage the processing time and thereby enhancing the performance of NSA.

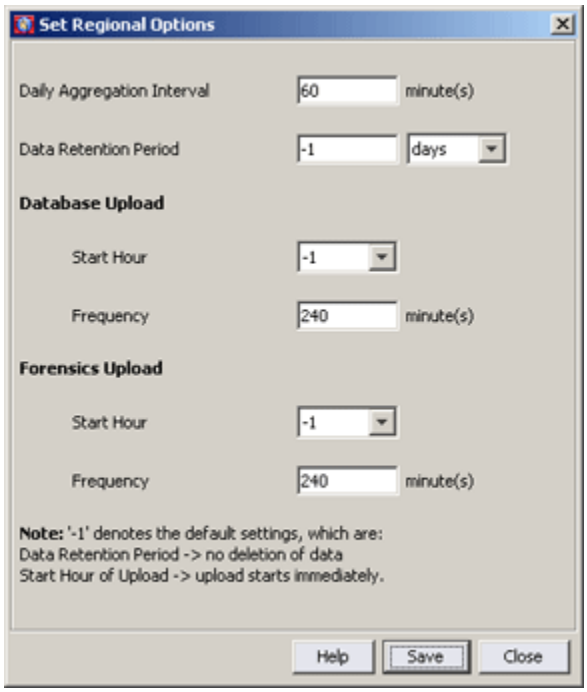


Options on Regional Server

On the Regional server, you can specify the time period for retention of data and the daily aggregation time interval.

Regional server processes the log data as part of load balancing activity and uploads it in the central database with reporting deltas and forensic deltas. From the **Set Regional Options** window you can specify the start time, frequency at which the Database and Forensic deltas are uploaded to the central server for each day.

NOTE: By default all the data is retained in the database, Database and Forensics upload is performed immediately unless specified by the user.



Monitoring

By default all the events from the regional are forwarded to the central server, Local monitoring and Alerting is turned off. Monitoring options on a regional server allows you to enable monitoring and alerting on the Regional server.

- **Forward events to Central**: This option is turned on by default and hence all events are forwarded to the Central NSA server where they are monitored. **Enable Local Monitoring**: Select this option to monitor SIEM data on the Regional server.
- **Enable Local Alerting**: Select this option to be alerted on changes and policy violations on the Regional.
- Click **Save**.

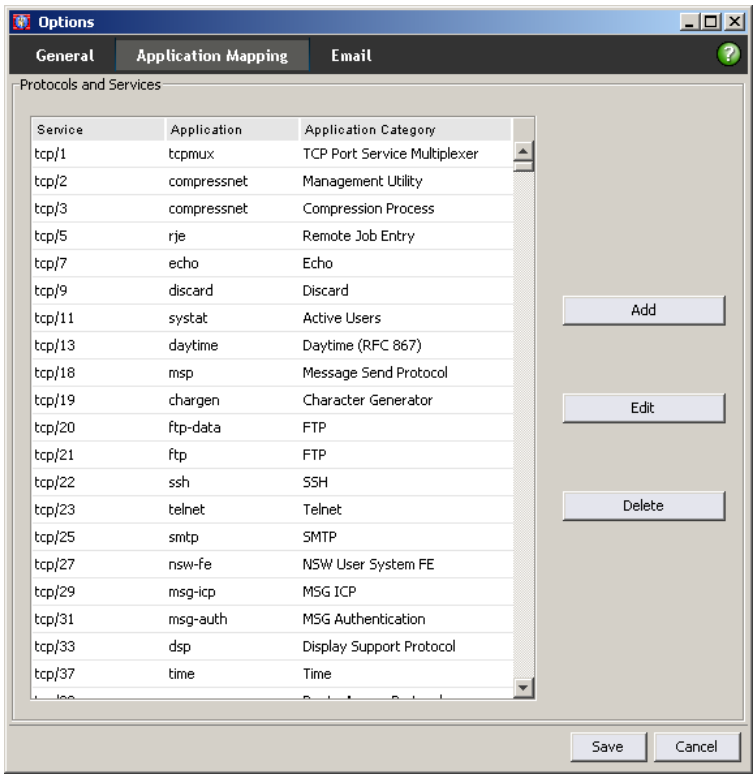
Security Center Options

Using this option in the General options window, you can select the options that are to be displayed in the Security Center. An admin user can apply these settings for all other NSA users or can limit these changes only to admin user account.

Application Mapping

The Protocols and Services list box displays all the services that will be analyzed and reported on by NSA according to the Application Category into which they are categorized. For instance, the service SMTP/25 is assigned to the category Simple Mail Transfer Protocol as this service deals with sending and receiving e-mails. You can add additional services and assign them to categories or new categories.

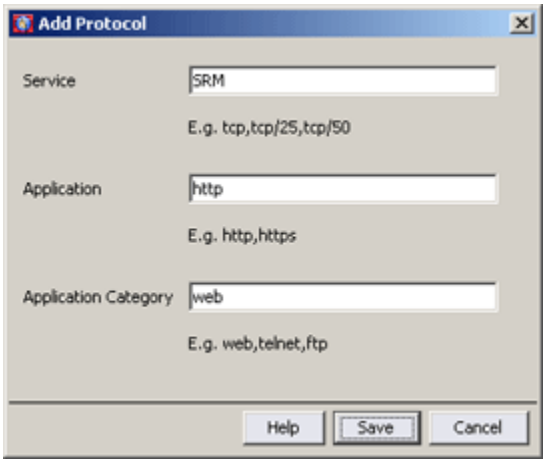
The Application Mapping Tab



To add a Service: Click **Add**. Enter the name of the Service and the type of traffic the protocol represents. For example, POP3 could be categorized under e-mail since it is a protocol used to send and receive e-mail.

- **Service**: Enter the name of the service.
- Enter the application name in the Application box.
- **Application Category**: Enter the name of the protocol category to which the service belongs.
- Click **Save**.
  You can see the service populated in the Protocols and Services list.

The Application Mapping Screen



- **To edit a Service**: Make any changes needed in the service name as necessary. The edited name should be exactly as you want it to appear in the NSA reports.
- **To delete a Service**: Select a service from the list and click **Delete**. This will remove the service from the Protocols and Services list.
- Click **Save**.

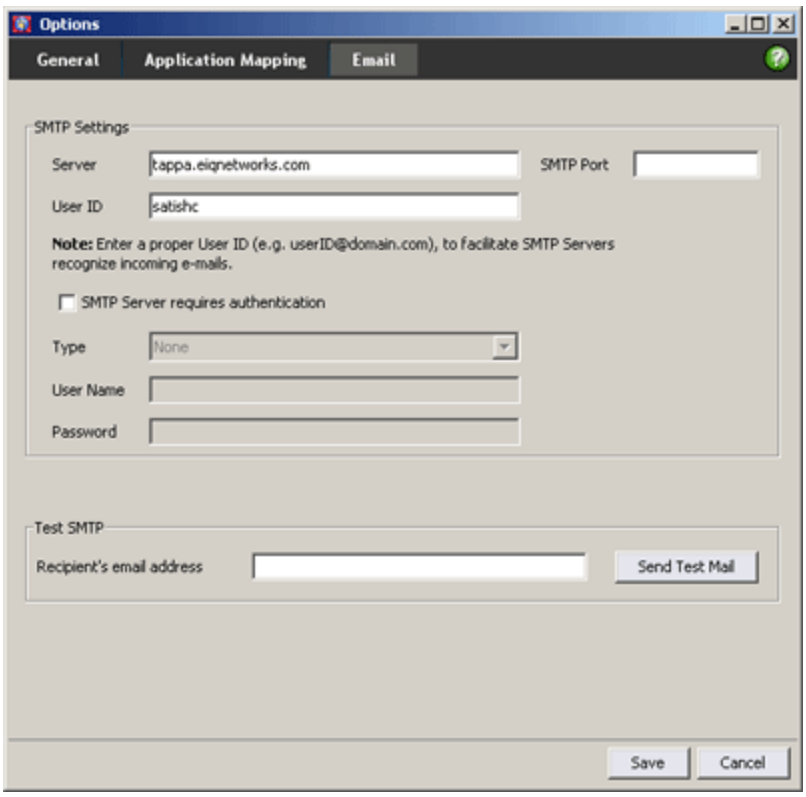
Note: The Added Protocol/service can be edited/deleted only from the **Options > Application Mapping** tab.

E-mail Settings

Enter the required information for your SMTP mail server in the appropriate boxes.

- **SMTP**: Simple Mail Transfer Protocol is a protocol for sending e-mail messages between servers. An e-mail client using either POP or IMAP can then retrieve the messages.
- **Server**: Domain name of the e-mail server supporting the Post Office Protocol (POP) protocol and saving mails e.g. www.hotmail.com.
- **User ID**: Enter the user name of the authorized administrator user ID.

The E-mail Settings Tab



- **SMTP Server Requires Authentication**: If your SMTP server requires authentication, select the SMTP server requires authentication check box and enter the server name and user ID in the text spaces provided.

  Follow the steps described below to specify the e-mail settings:
  - Specify the authentication type to login to the SMTP server from the Type drop-down list.
  - Enter the **User name** and **Password**.
  - Specify the **SMTP** port number in the SMTP Port box.
  - Click **Save**.

- **Test SMTP**: To verify your SMTP settings, you can send a test mail to the intended recipient by entering his e-mail ID in the **Recipient's mail ID** box. Click **Send Test Mail** button.

Chapter 8: Reports Catalogue

In the Reports Catalogue, you can view all the reports that are available in NSA categorized and arranged systematically. The Super Admin can decide which reports have to be made available to all users including him, by using this option.

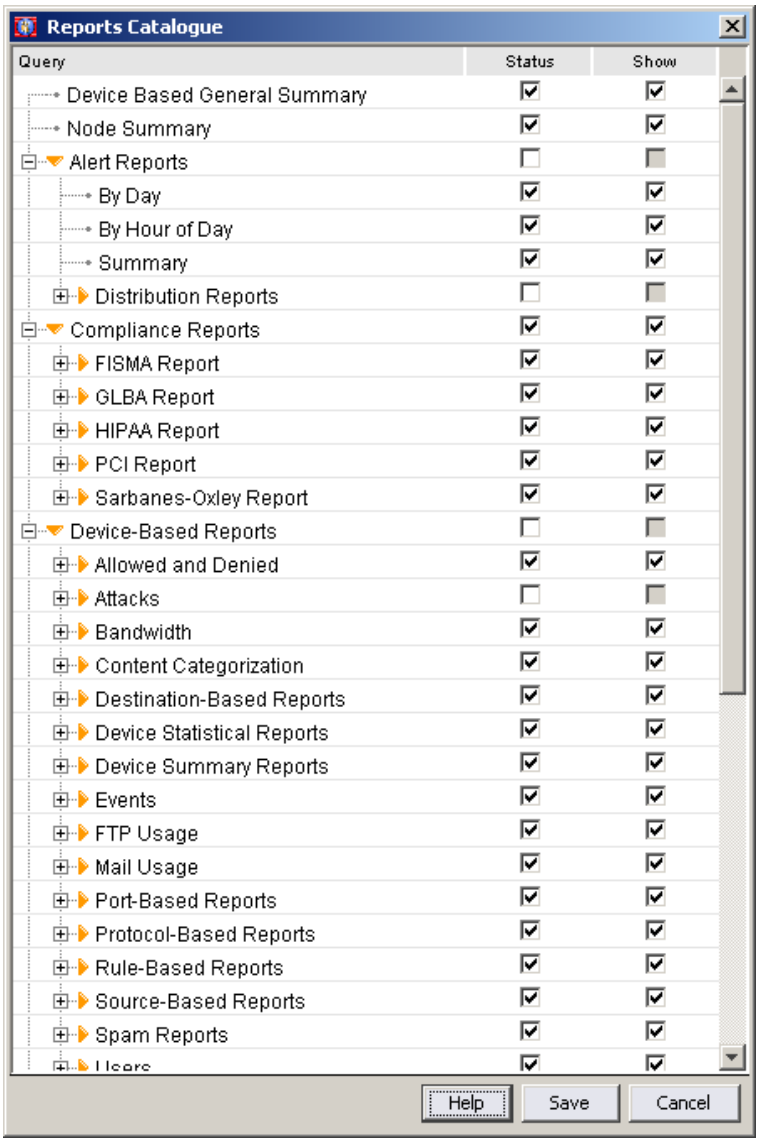
Selecting Reports

By default all the reporting sections are accessible to the users. Being a Super Admin you can restrict the reporting ability of NSA users by de-selecting the reporting sections. For example if you want to restrict Alert based reports, uncheck Alert Based Reports from the Reports Catalogue. When any of the user logins and tries to report on this module/query, a message is displayed that Super Admin has disabled the report.

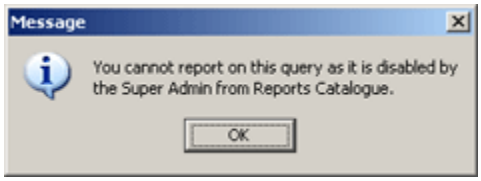
NOTE: Factory default settings of NSA disable some of the queries within the reporting sections.

Follow the steps given below to select Reports to be made available across the application for all users:

1. From the main window, click **Options** and select the **Reports Catalogue** option.
2. The Reports catalogue window opens displaying all the available query reports.
3. Each query/section is associated with **Status** and **Show** columns.
4. When the **Status** of the query is selected, then the respective query/section is enabled.
5. When **Show** option is selected, then the respective query/section is displayed in the **Security Center > Reports** module.
6. Click **Save**.



7. The settings will be reflected in all the modules where reports are displayed including the Security Center. If the user tries to open a report that has not been selected on the **Reports Catalogue** by the Super Admin, the following message is displayed:



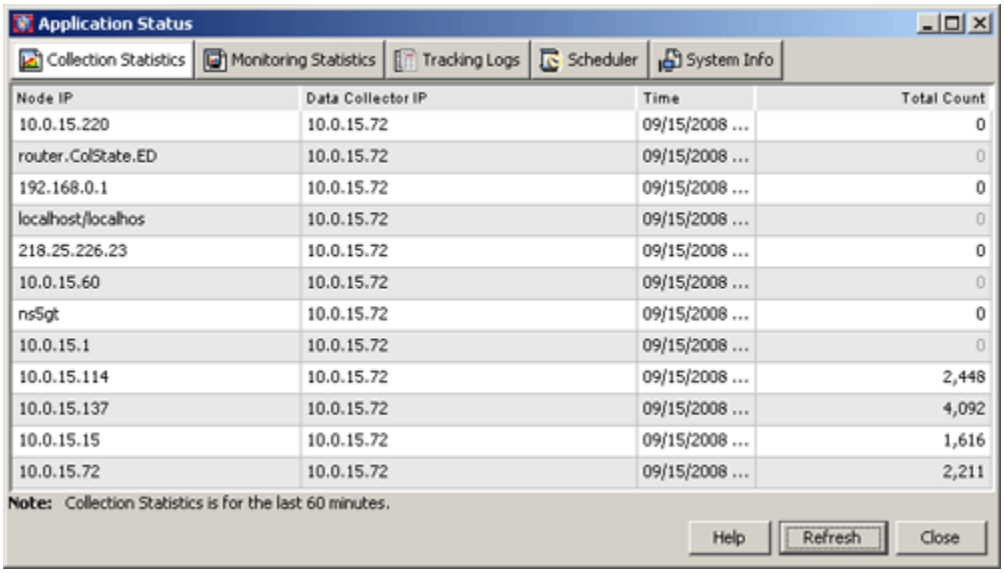
Chapter 9: Status

The Status (Application Status) screen displays information on various components that are important to manage and keep the NSA up and running. You can view information about the delta files transmitted from the Data Collector. It also provides you with information on the status of log files, device IPs, log file names, last updated date and time, file sizes, components required by NSA for the installation, and scheduled tasks.

The Application Status screen provides information on the following.

Collection Statistics

This tab displays details of the Data Collector service of a regional data collector that includes:

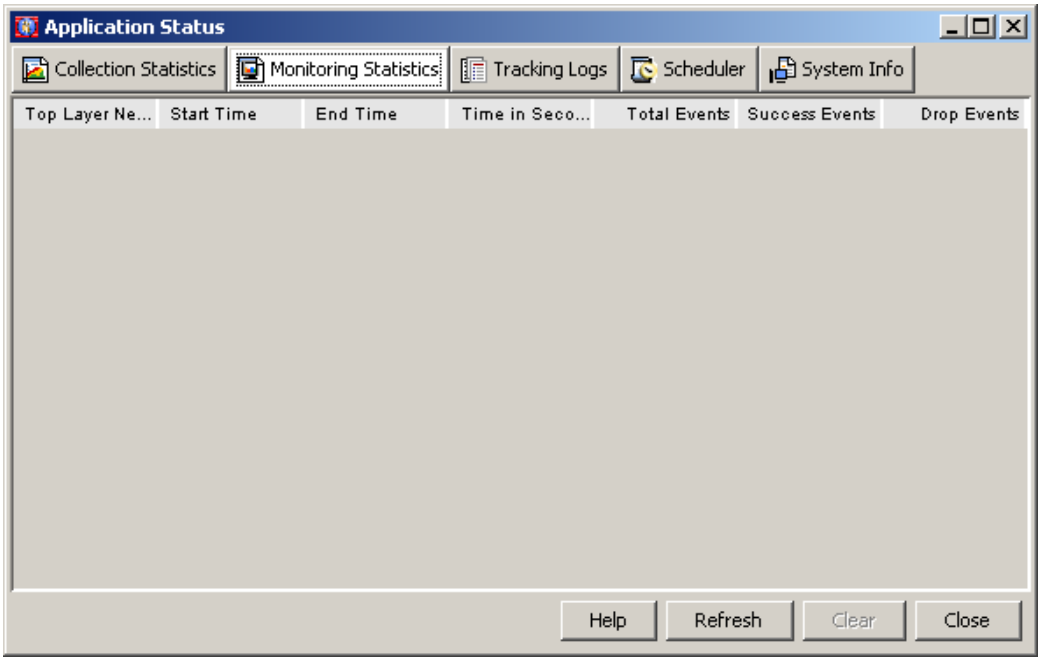


- **Node IP**: Displays the IP address of the nodes which are configured to NSA Data Collector.
- **Data Collector IP**: Displays the IP address of the Data Collector for which the statistics are being displayed.
- **Time**: Displays the start time when collection began after the recent refresh interval.
- **Total Count**: Displays the total number of events parsed.
- Use the **Refresh** button to update the status of statistics displayed for the Data Collector.

Monitoring Statistics

This tab displays details the monitoring statistics by a regional server that includes:

- **Corero Network Security Analyzer IP**: Displays the IP address of the device on which the NSA Regional is installed.
- **Start Time**: Displays the start time when monitoring began.
- End Time: Displays the end time where the monitoring has finished.
- **Time in Seconds**: Displays the total time in seconds, for which these statistics are displayed.



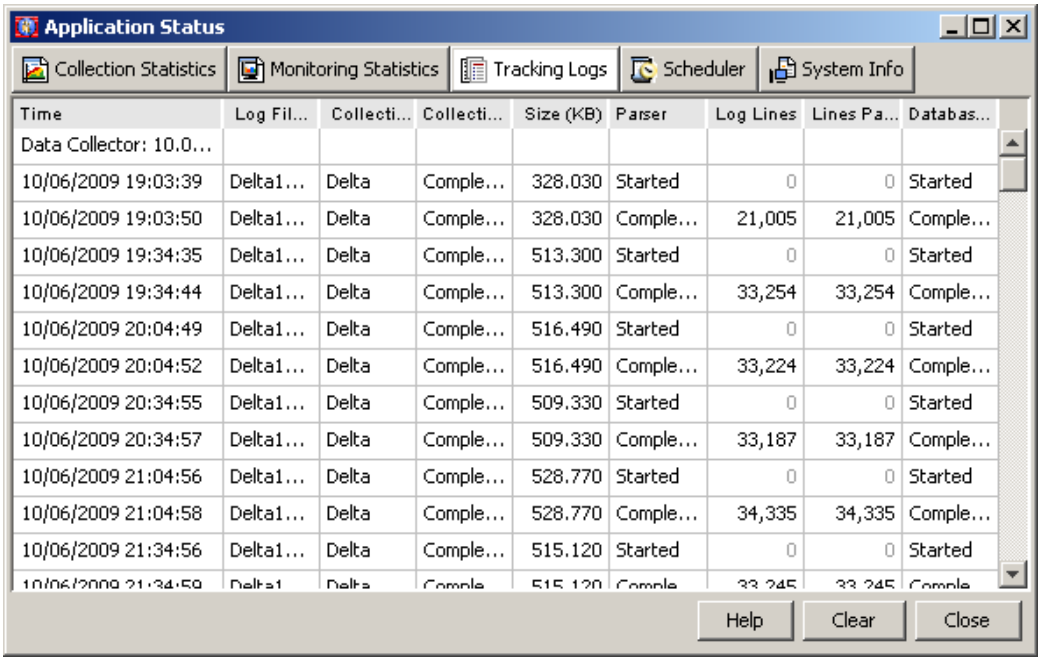
- **Total Events**: Displays the total number of events monitored in a given time period.
- **Success Events**: Displays the total number of events successfully monitored in a given time period.
- **Drop Events**: Displays the total number of events dropped in a given time period.

  Use the **Refresh** button to update the status of statistics displayed for Monitoring module of the regional server.

Tracking Logs

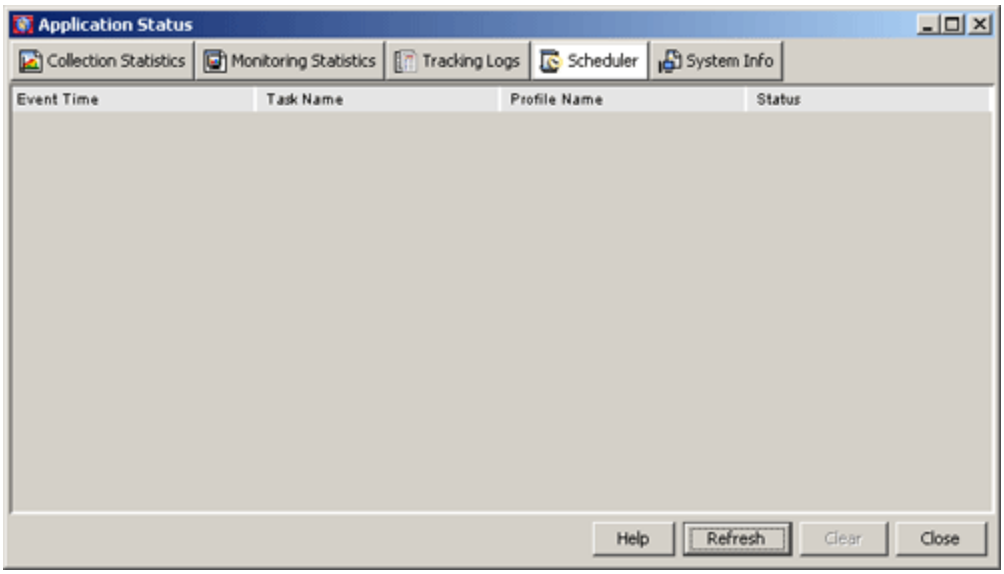
This tab displays information on the delta log files successfully received by NSA from a Data Collector and updated to the database. If a single delta file saves records of multiple devices, corresponding device names are displayed. The following information can be viewed on the App Status screen:

- **Time**: Timestamp of when the status "event" occurred.
- **Log File Name**: The name of the log files.
- **Collection Method**: Displays the File collection method for example log Delta, FTP, Local File etc.
- **Collection Status**: Informs you the status of log collection for example:
  -Started collecting from ftp://ftp.mysite.com
  -Completed
- **Size (KB)**: This is the total size (in Kilobytes) of the file that was collected or fetched.
- **Parser**: The status of parsing activity is shown here as Started, Completed, or Failed.
- **Log Lines**: Displays the total number of lines in the log file.
- **Lines Parsed**: Displays the Total number of lines that were successfully parsed. The number of lines that could not be parsed can be calculated from the Log Lines minus Lines Parsed.
- **Database Update**: The status of Update is displayed as Started, Completed, and Failed.
  Use the **Clear** button to delete content about old log files so that the details of new log files updated to the database can be displayed.



Scheduler

This tab provides information on the status of the regularly scheduled tasks configured for different profiles. The Scheduler records a history of how an event fares when it runs — whether it runs successfully or not, what errors, if any, occur and related information. It provides you with an overview of the tasks and their schedules. It contains a listing of all the reports scheduled to run, the profiles they are associated with, and their status. Use the **Clear** button to delete all the old events and display only the latest events created by the Scheduler tasks.

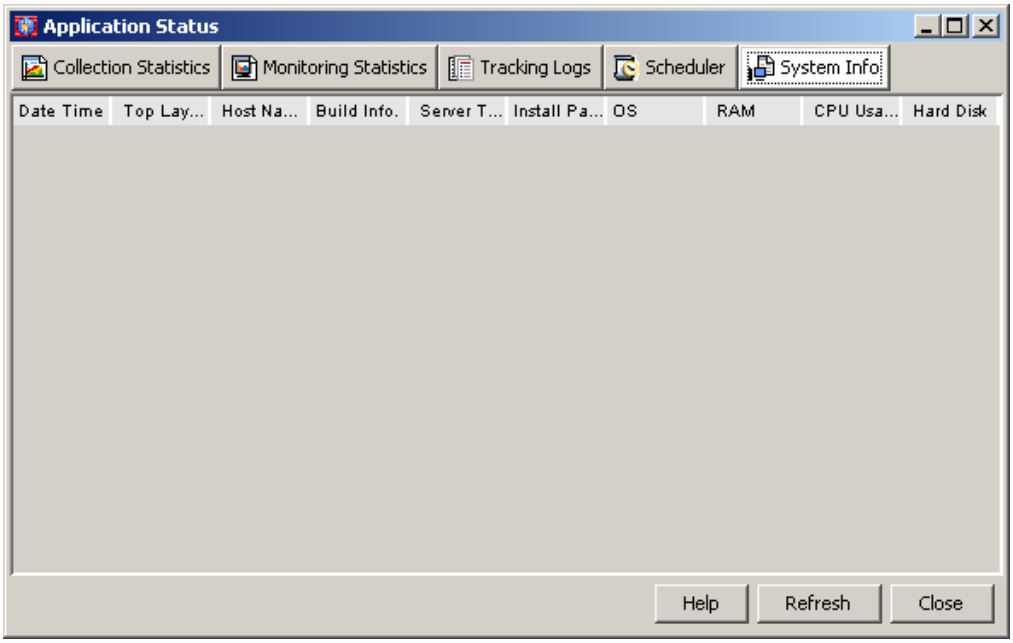


- **Event Time**: Lists the date and time on which the scheduled report generation started.
- **Task Name**: Lists the name of the task generating the report.
- **Profile Name**: Lists the profile name associated with the task.
- **Status**: Reports whether the task ran successfully or that one or more errors occurred. The error messages will explain any problems that the scheduled events encountered. This column also reports whether the scheduled report has been mailed and/or uploaded to ftp site.

NOTE: Only Administrators and Power users have access to App Status information.

System Info

This tab displays details of the following:



- **Date Time**: Displays the timestamp of when the status event occurred.
- **Corero Network Security Analyzer IP**: Displays the IP addresses of the central or regional to which this device is configured.
- **Host Name**: Displays the hostname of the system.
- **Build Info**: Displays the build number of the NSA which is currently installed on this system.
- **Server Type**: Displays if the server type is of Central or a Regional.
- **Hard Disk**: Displays the information of total disk space and available disk space for each drive on the system and also the type of file system existing on this drive.
- **OS**: Displays the operating system of the system running NSA server.
- **RAM**: Displays the value for size of RAM on this system.
- **CPU Usage**: Displays the value for percentage of CPU resources used for accomplishing a given task.
- **Install Path**: Displays the path where the NSA server is installed on this system.
  Use the **Refresh** button to update on any changes in the system information.

Chapter 10: Users

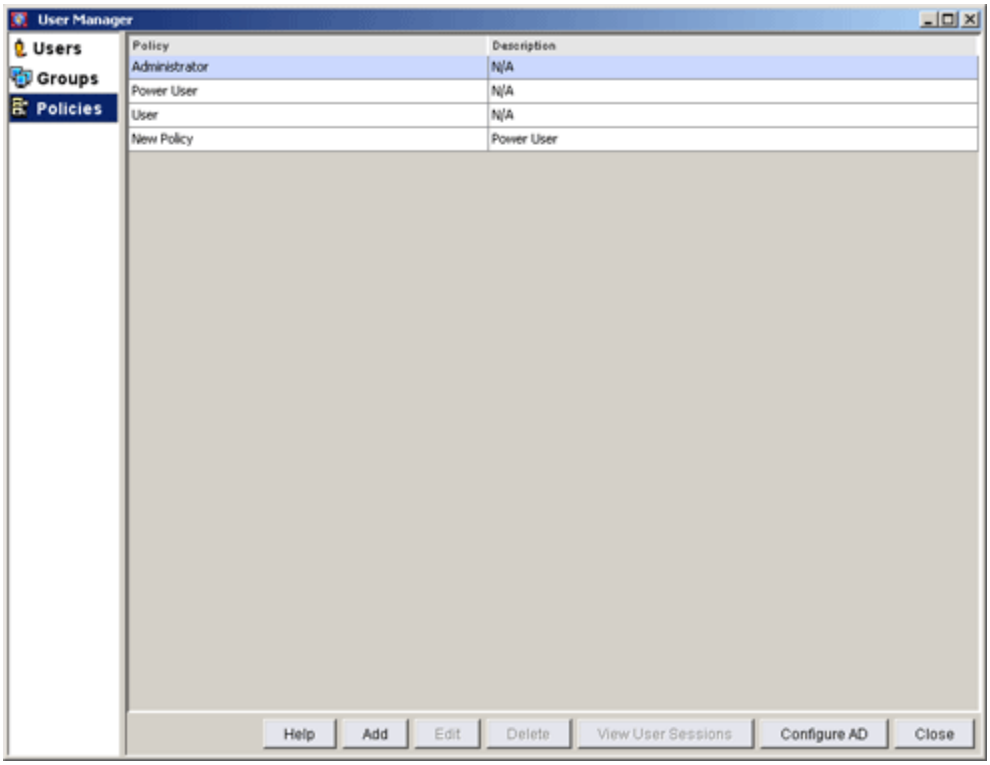
You can create users with different access rights through the User Manager. This helps you manage and ensure security of your profiles and associated policy settings.

IMPORTANT: Only an admin user can access User Manager.

User Manager UI in NSA 5.1 mainly comprises of the following 3 categories:

- Users
- Groups
- Policies

User Manager Main Screen

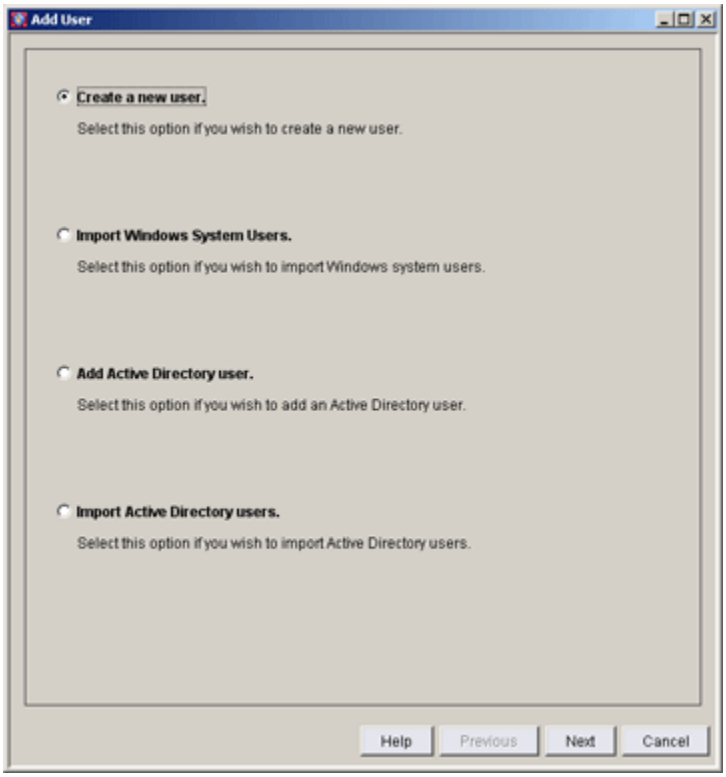


Users

An administrator can create Administrator, User and Power User accounts. If you are a default admin user, then you have access to all the modules of the application. Power user can access all the other functionalities except Devices, Groups, Users, Licenses and Status. But his scope is defined by the administrator. A User (Report user) can only run and view all/some of instant reporting sections as specified by the administrator.

You can add new user accounts to NSA by the following ways:

- Create a new user
- Import Windows System Users
- Add Active Directory User
- Import Active Directory users



Create a New User

NSA provides three levels of access rights: Administrator, Power User and User.

Each of the user types and the rights given are discussed below:

Administrator: There can be only one Super Administrator to manage the entire application with exclusive rights to control, create, delete, and edit even other users with customized privileges.

Power User: Users in this group can be classified as read-only admins. They cannot manage Devices, Groups, Users and Licenses. The Power User can create, edit, delete and view profiles, however, access to Collection-based policies and generation of file-based profiles is restricted.

User: User accounts in this group can only generate all or few instant reports sections depending on the privileges assigned in the user policy. While creating a policy, the Super Admin can specify the report categories of devices accessible to the users associated with the

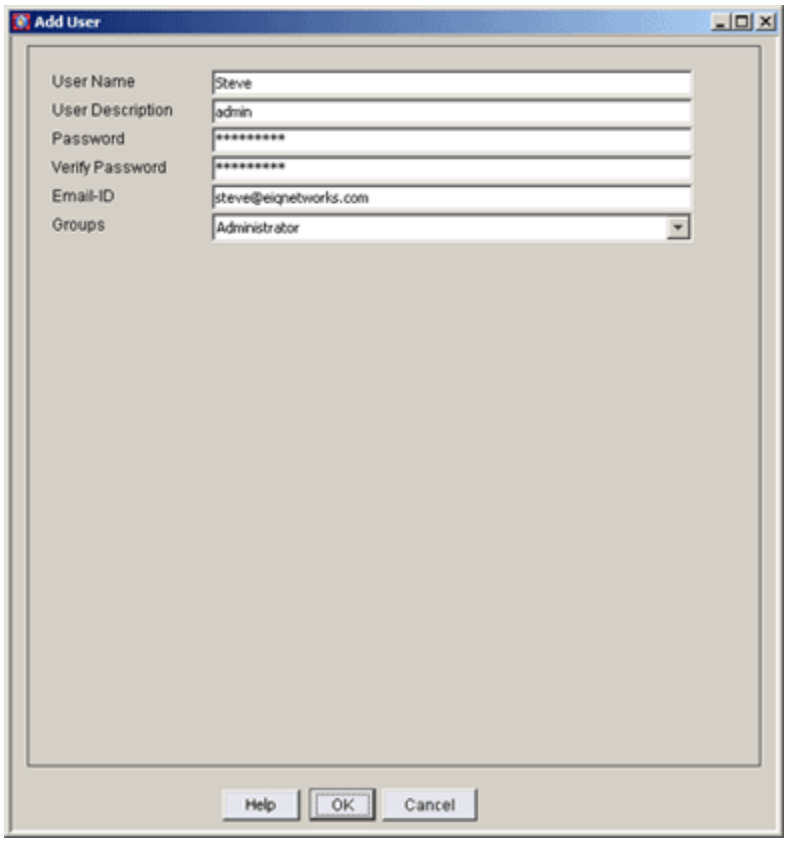
policy. The Super Admin can also specify ACLs during creation of user policies to control the portal-access and right-click-menu access. Note that there are separate reporting sections for devices.

Follow the steps described below to add a user:

1. On the main screen, click **Setup > Users** option. The User Manager screen opens.
2. Select the **Create a new user** option and click **Add**. The **Add User** dialog opens.
3. Specify a login name for the user in the **User Name** text box.
4. Specify the description for the user account you want to add.
5. Enter the corresponding password in the **Password** text box and re-enter it again in the **Verify Password** text box.
6. Specify the valid e-mail ID of the user.
7. From the **User Group** drop-down list, select a group that defines the privileges for the user.

   If you are creating a Power user then you need to specify the device groups and devices that the user should have the privilege to access and report on, and for a report User you need to specify the device groups and the report categories that the user should be able to generate reports on.
8. Click **Save**.

NOTE: Any Normal User account carried forward from previous versions of NSA is categorized as Power User which is non editable and cannot be deleted.



Editing a User

While editing a user on the Edit User screen, you can change all of the available fields except the **User Name**.

Import Windows System Users

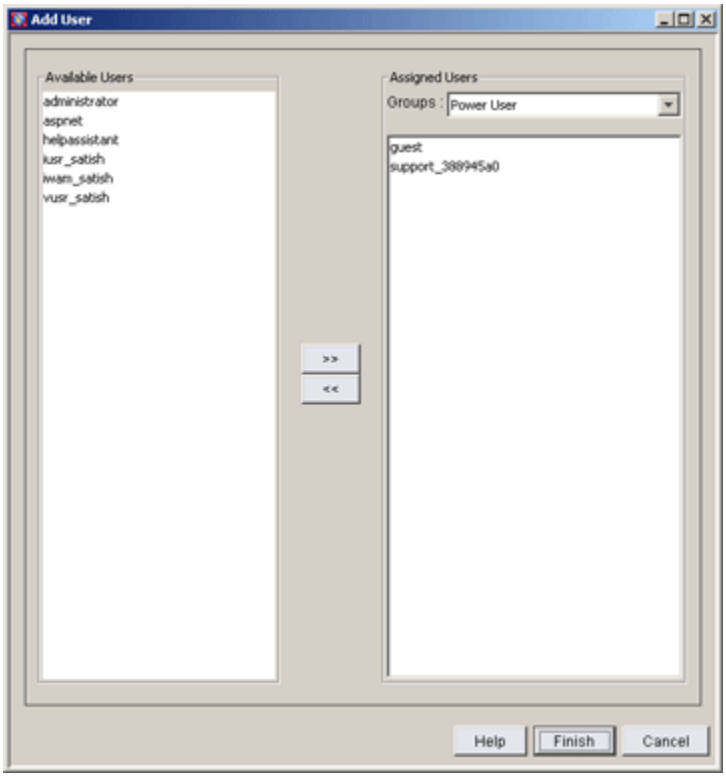
Native OS user authentication allows you to leverage single sign-on thereby eliminating the need to maintain separate security credentials.

NOTE: You can only import the user accounts present in the windows operating system.

To create and import a new windows user account into NSA, define a new user for Windows operating system from Control Panel> Administrative Tools > Computer Management >System Tools > Local Users and Groups.
The user account that you have just created is displayed in the Add User window and can be imported into the NSA application.

Importing User Accounts from Windows Operating System

1. Select **Import Windows System Users** from the **Add User** wizard. Click **Next**.
2. A window is opened displaying all the existing user accounts from the windows operating system.
3. Select the User accounts that you want to import into NSA and into which Group.
4. Configure at least one device for the user on which the user can monitor or report on.
5. Click  icon to move the user into the assigned user list.
6. Click **Finish**.



NOTE: By default users cannot report on any devices. Administrator must grant them the privilege to access device and report sections.

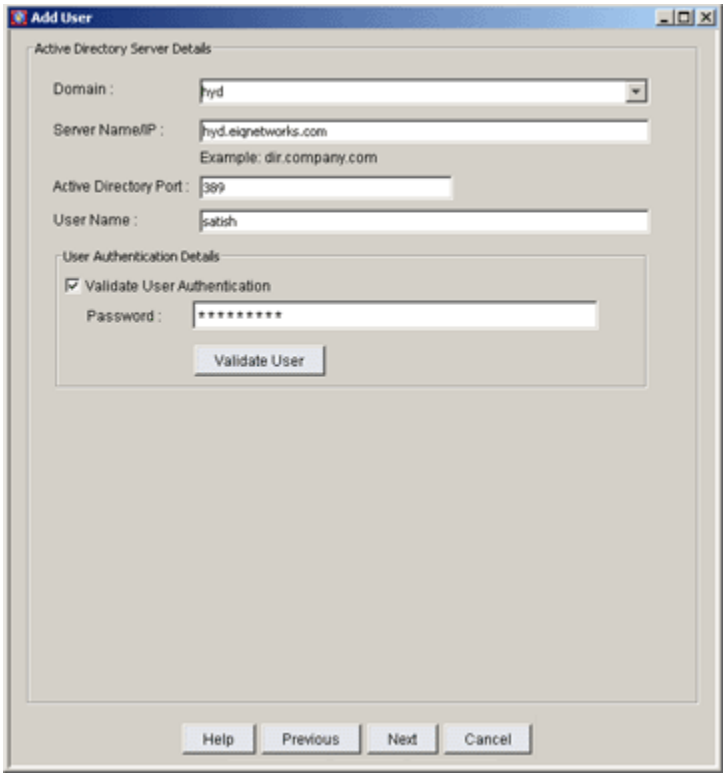
Add Active Directory User

Important: Configure your Active directory Server details before adding any active directory user accounts to NSA.

NSA has the facility to add a new domain user into specific groups. In this case no domain privileges are necessary and you can directly add a new user with the domain account credentials.

Add Active Directory User:

1. Select **Add Active Directory User** wizard. Click **Next**.
2. A window is opened where you need to enter the active directory server details.
3. Specify the name of the **Domain** and the **Server Name / IP** of the domain.
4. Enter the Active directory port for the server. By default port 389 is used in connecting to AD server.
5. **Optional Settings**: Specify the User Name and Password for the new user account using which the respective user would login into the NSA application. Click **Validate User**. This is used to check for authentication.
6. Click **Next**.



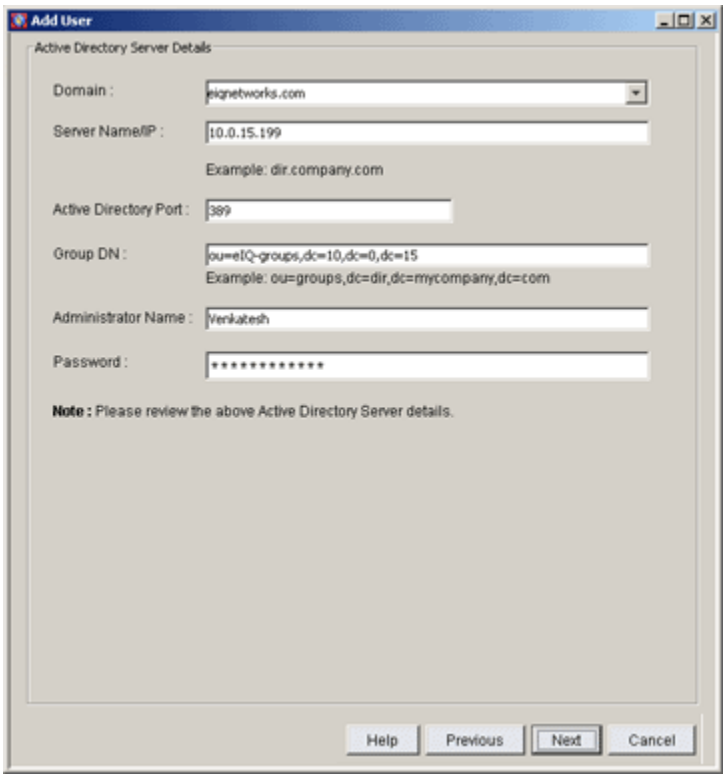
Import Active Directory Users

NSA supports the use of an external LDAP-enabled directory to authenticate and authorize users on a per group basis.

LDAP group-based authentication for the NSA Appliance can be configured to support Microsoft Active Directory by keeping the authentication centralized on your directory, a security administrator can always know who is accessing network resources and can define user/group-based policies to control access.

Active Directory natively supports a fully integrated public key infrastructure and Internet secure protocols, such as LDAP over SSL, to let information being accessed beyond their firewall to extranet users.

IMPORTANT: Configure your Active directory Server details before you import its user accounts to NSA.



Importing Active Directory Server User Accounts:

1. Select Importing Active Directory Server Users from the Add User wizard. Click Next.
2. A window is opened displaying all the existing user accounts from the Active Directory server.
3. Select the user accounts that you want to import into NSA and into which Group.
4. Click  icon to move the user into the assigned user list.
5. Click **Finish**.
6. It is recommended to install NSA with LDAP authentication if your environment is distributed.

   Important:

   - Windows OR Active Directory user account passwords should not contain '&' ampersand character in them. Since logging into NSA is not possible with such accounts, password credentials for those accounts need to be reset before importing them.
   - While importing Windows OR Active Directory users into the existing groups of NSA, users imported to groups other than Administrator, application will notify you to assign devices which the newly imported user can monitor and report on.

   Click **Assign Now** button. The **Configure New User** window displays.

Refresh

You need to click the **Refresh** button when you want to re-populate the user list in the modules that seek user information from the User Manager.

User Sessions

Click **View User Sessions** to open the **User Sessions** screen. This screen records a history of users accessing NSA and provides you an overall view of the user activity. It enlists all the users who logged on to NSA, the client machine name and the data and time they logged in. The admin user who has currently logged in can clear all the recorded user sessions by clicking the **Clear Sessions** button.

- **Status**: This reports the operation (login or logout) that the user performed.
- **User Name**: This lists the user name with which the user logged on to NSA.
- **System**: This lists the client machine from which the user logged on to NSA.
- **Date**: This lists the date and time on which the operation was performed.

NOTE: NSA gives the ability to time-out a user-session thereby forcing the user to re-login. TimeOut settings can be specified through a configuration parameter UserSessionTimeOut=<min> in fwaconfig.ext file found in the installation path. By default the value is set to as NO-EXPIRY.

Configure AD (Active Directory)

Click **Configure AD** button on the main screen of the user manager, the **Configure AD Server Details** screen opens.

Add Active Directory Server Details:

1. Click the **Add** button to add the details of your active directory server.
2. The **Add Active Directory Server Details** window opens.
3. Provide the Domain, Server Name/IP of your domain server and the Active Directory port, Group DN details of your server accordingly.
4. Click **OK.**
   Details are validated and on successful validation, the domain is added in the **AD Server Details** window.

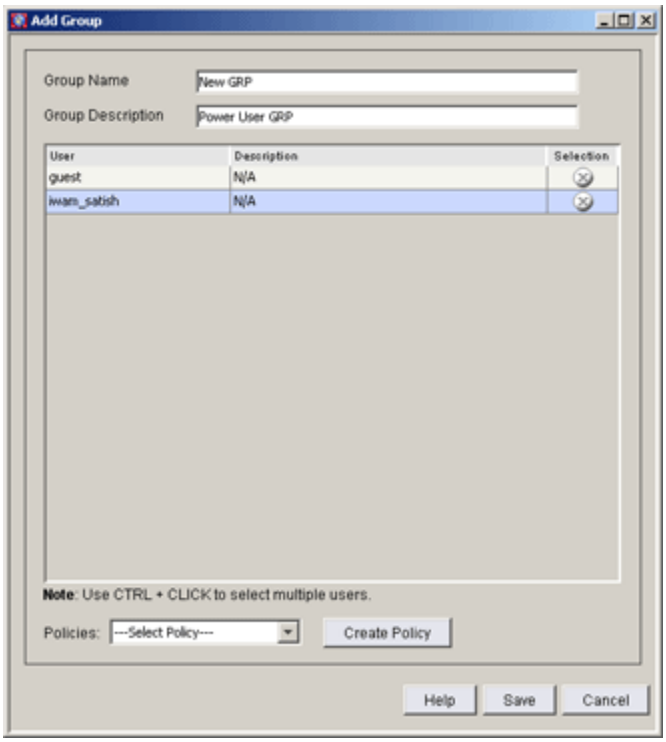
Groups

Using the **Groups** option, an administrator can create and define policy bound users who will be a part of the group. You can even select to define a policy from the Groups option which subsequently can be associated with the users who belong to the selected group.

Add Group

Using the **Add Group** wizard, an administrator can create a group, add existing users to the group and also associate policies.

1. Specify a Group Name that you want to define and give an appropriate Group Description.
2. Add Group window lists all the existing user accounts added in the application.
3. Select the users whom you want to make part of this group.
4. Select a policy you want to associate with from the **Policies** drop-down list or define a new policy for the group.
5. Click **Save**.



Policies

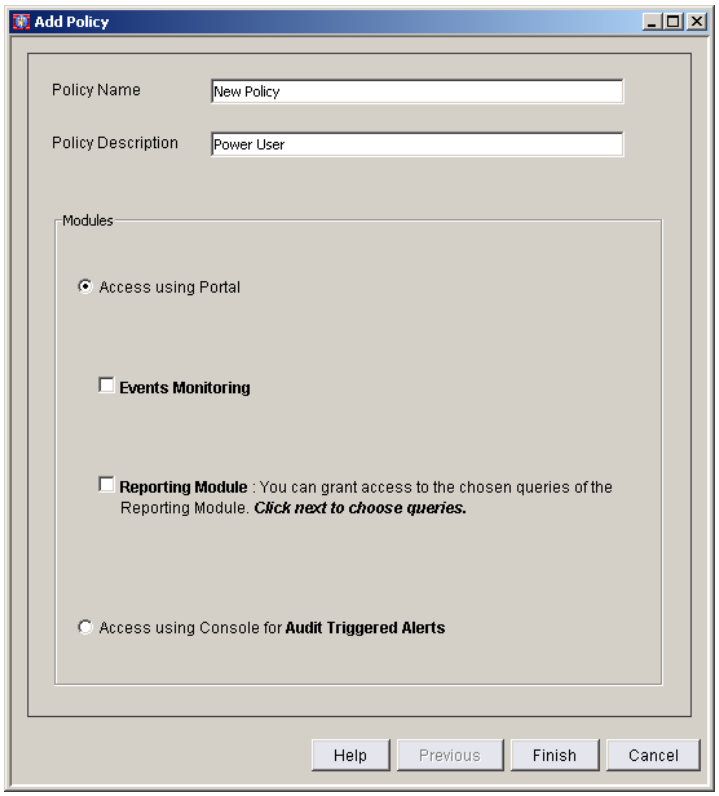
Using the policies option, an administrator can define the criteria on granting permission to use the following:

- Modules
- A Console user and audit triggered alerts

Add Policy

Follow the steps given below to define a policy by using the Add Policy wizard:

1. Specify a Policy Name that you want to define and give an appropriate Policy Description.
2. Select the modules which a user can access if associated with this policy. Modules available for the user are:
    - Access Using Portal
        - Events Monitoring
        - Reporting Module
    - Access Using Console for Audit Triggered Alerts



3. **Access Using Portal**: If **Reporting** module is selected, click **Next** and the query selection screen opens.
4. Select the query sections that a user associated with this policy could report on.
5. **Access Using Console**: If this module is selected, only triggered alerts can be audited.
6. Finally, click **Finish**.

Audit Triggered Alerts

Using this option, admin user has the option to create a user account whose sole priority is to monitor the alerts generated for a specific user.

Creating and assigning privileges to an Audit User

1. Create a Power user account from the user manager.
2. Create another user account (**Audit User**) that is only created to monitor/audit the alerts triggered for the policies created by the sample user.
3. While assigning a policy, select **Access using Console** module and select the user (created in step 1) from the drop-down list for which the Audit User account will monitor and acknowledge the triggered alerts.
4. When the **Audit User** (created in step 2) logins to the application, he/she would be able to audit and acknowledge the alerts triggered by the policies created by the Sample user.

IMPORTANT: After upgrading to NSA 5.1 on a multi-language support enabled system, admin user has to reset passwords of all such user accounts that contained special characters. If the admin user password also contained special characters, obtain a new UserManager.xml from the Corero support team with a new password defined for the administrator.

Change Password

As a non-admin and non-power user (Audit User and User), you can change the login password by following the steps given below:

Click on the  icon present on the right top corner of the portal, a drop down menu with the following options is displayed:

- About
- Help
- Change Password
- Logout

Select Change password from the menu list and the following change password window opens:

1. Enter the current password in use in **Old Password** text box.
2. Enter the desired password that you want to change to, in the **New Password** text box.
3. Re-enter the desired password in **Verify Password** text box.
4. Click **Save** and re-login into the application for the password change to take effect. Else, click **Cancel** to abort the task.

Chapter 11: Manage

To manage the Devices you have the following tabs:

- Groups
- Devices
- Policies
- Profiles
- Forensics

Only an admin user can access the above mentioned tabs.

Groups

The Groups screen displays the list of groups you created and the devices under each group. You can add, edit and delete groups from this screen. You can create local groups and global groups that help administrators manage all the devices in the network through one window.

Devices

The Devices screen lists your data collectors/manually added devices. You also can add or delete a device/virtual device on this screen. Define Collection Policies for devices.

Policies

In NSA a policy is a formal set of rules to define the course of action that the user needs to take under specific circumstances. A rule can dictate— which nodes to consider, what event type to filter or negate, which entities with what values to add and so on. A policy is created on the customized device or the existing rule templates. On implementation of a policy the user can classify the Policy under an Event class by associating it to a report query. A user can add, edit, copy or delete a Policy.

Profiles

Profiles also allow you to generate user specific reports where in you can apply filters to narrow down your data collected from various configured nodes, to the information you need most in the desired type and format, which can save time and resources. Profiles are created through a wizard. When the wizard has completed the profile appears in the profile list.

Forensics

NSA provides an easy-to-use forensics search engine that allows you to quickly sort through the archived logs. Forensics analysis helps you to vector security breaches and ensure compliance by detecting anomalies, identifying policy violations and displaying a chronological order of malicious activity.

Chapter 12: Node Management

This section describes how to manage your devices and NSA Data Collector. Once the Data Collector is configured, NSA will access device logs using the syslog service for processing and storage. Log file data is stored either in the built-in database or an enterprise database. To manage the Devices, the following two tabs can be used which are present on the main menu:

- Groups
- Devices

Once any Device gets associated with NSA it is assigned a unique symbol for easy identification. The following table gives the details of the symbols used in the Groups/Devices screen display:

	Represents a configured licensed device.

The Groups Screen

The Groups window displays the root information about the node where NSA is installed and the default group under it. The default group comprises of all the Devices that are configured to NSA. The devices can be identified by their unique respective icons. You can create separate groups based on criteria like - location, department, and importance to manage all the devices in the network through one window. You can also add or delete groups from here.

The Default Group

The default group is automatically created by the NSA. You can also create new group and allocate devices under that group. If you delete a group, all the devices in that group are automatically shifted to the default group.

Adding a Group

Follow the steps described below to add a group:

1. On the **Groups** screen, click **Add**. The **Add Group** screen opens.
2. Enter a name for the group in the **Group Name** box.
3. Select the parent group from the **Sub-Group of** drop-down list, if you want to create a Sub-group under any previously created Group.
4. Select the devices you want to add to the group and click **Finish.**

Editing a Group

Follow the steps described below to edit a group:

1. On the **Groups** screen, select the group you want to edit and click on **Edit Group**. The **Edit Group** screen opens.
2. Select the devices you want to add or remove from the existing group and click **Save**.
   Note: Default groups cannot be edited.

Editing the Asset Value of a Group/Device:

When you add a new device, it is automatically placed under the **Default Group** with the default asset value as 10. NSA admin user can change the asset value considering its importance ranging from 5-1000. Based on this value Risk Score for a device is calculated.

Editing the Device asset value:

1. Click the **Groups** tab. The Groups screen opens.
2. Double click on the Asset Value associated with a device.
3. Provide the new value assessment for the device ranging from 5-1000 given its importance.

Editing the asset value of a Group:

1. Click the **Groups** tab. The Groups screen opens.
2. Right-click on the Group, Select **Set Asset Value** option to change the asset value associated with it.
3. Provide the new value assessment for the group ranging from 5-1000 based on the importance.

Important: Individual Asset values of devices will be overridden with the Group Asset value when the asset value of each device/host within the group is less than the Group Asset Value.

Moving a Device from Default Group

When you add a new device, it is placed under the Default Group. You can move the added device from the default group to any other existing group by following the steps described below:

1. Select the **Groups** tab.

2. Click on the group to which you want to move the device. A screen that lists all the devices is displayed.
3. Now select the device you want to move under the selected group.
4. Click **Save**.

Right-click Options

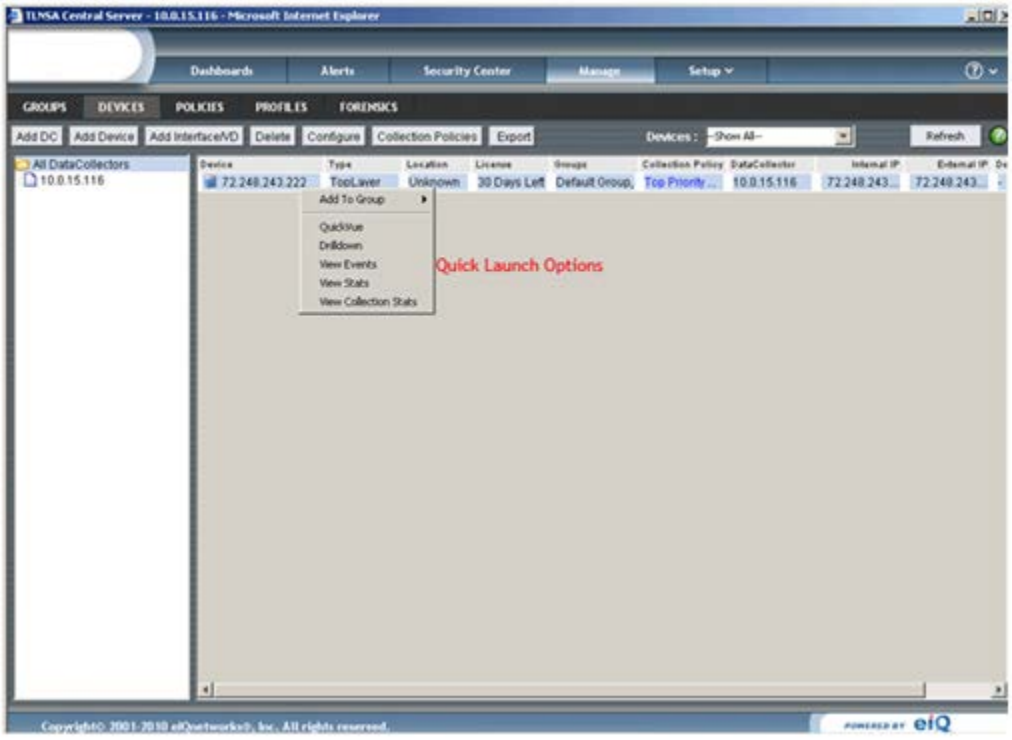
Right-click on Device, a pop up displaying the Options available for a device based on your selection.

- Context Sensitive Right-click options for Devices

The Devices Screen

The Devices screen lists the Data Collectors, configured/un-configured and manually added devices. You also can add or delete an un-configured device/virtual device from this screen.

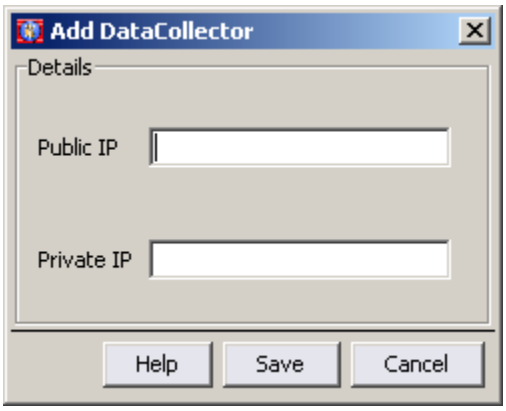
Devices Screen



Add DC

Before you install a Data Collector, NSA administrator should first add the DC from Manage > Devices tab by providing the Data Collector host's public & private IP addresses.

Important: If the DC IP is not added at the Central, installation of DC will not be completed.



Follow the steps described below to add a DC (Data Collector):

1. Click on the **Add DC** button from the Devices tab. The **Add Data Collector** window opens.
2. Enter the public & private IP addresses of the host where NSA Data Collector will be installed.
3. Click **Save**.

Adding a Device

Follow the steps described below to add a device:

1. On the **Devices** screen, click **Add Device**. The **Add Device** wizard opens.
2. Select an identifier by which you want your device identified. A device can be identified either by its external IP address, internal IP address, or device ID.
3. Enter the device name in the **Device** box.
4. Select the device type from the **Device Type** drop-down list.
5. Enter the location in the **Location** box and click **Save**.

NOTE: To display an unconfigured in the **Add Device** window, click on the IP of the device under the Data Collector or under the Manually Added Devices and click **Save**.

IMPORTANT: If the device is of type Intrushield, you need to perform the following configuration changes to obtain reports from the Intrushield device.

Configuring the Intrushield devices

To enable NSA Server generate reports on the log events streamed from the Intrushield devices, edit the intrushield.ext file found in the application path (you path ...\CoreroNSADataCollector) folder.

1. The file has the following information:
   <device IP> <Column names>
2. Format of the IntruShield device log columns must be separated by a semicolon and each column Identifier would begin and end with $.
3. Edit the device IP column with the IP address of the Intrushield device which is streaming data to the NSA Server via Data Collector. For example 192.168.1.99 is the Intrushield device IP address that you want to report upon, uncomment <device IP> tag and provide the respective IP address as <192.168.1.99> with respective columns in the intrushield.ext.
4. To report on more intrushield devices, append the intrushield.ext file with the device IP and respective Intrushield columns to be included in the report.

NOTE: NSA supports McAfee Intrushield logs collected by the Data Collector and not from the Log File as the data source option.

Adding a Virtual Device or Interface

Follow the steps described below to add a virtual device:

1. Select a primary device from the devices list and click **Add Interface/VD**.
2. To add a virtual device or interface, select any one of the available options:
   - Virtual Device
   - Interface
3. Select Virtual Device and enter the IP address of the virtual device and click Save.

   NOTE: A primary device must be selected to monitor its virtual device or an interface.
4. Select Interface and specify the Interface Direction.
   - Internal
   - External
5. Enter the IP address of the Interface and click **Save**.

NOTE: Interface name will have the prefix as Iface-.

Deleting a Device

Follow the steps to delete a device:

1. Select the device/s that you want to delete.

   Note: By default, all devices that are not configured on the NSA Data Collector are selected.

2. Click **Delete** to delete the list of devices.

   TIP: Deleting a device will also remove data pertaining to that device from the database.

This device is now displayed under the category Unconfigured Devices.

NOTE: The ability to dynamically add or delete a device is important for MSSPs who often keep adding and deleting devices.

Configure Devices

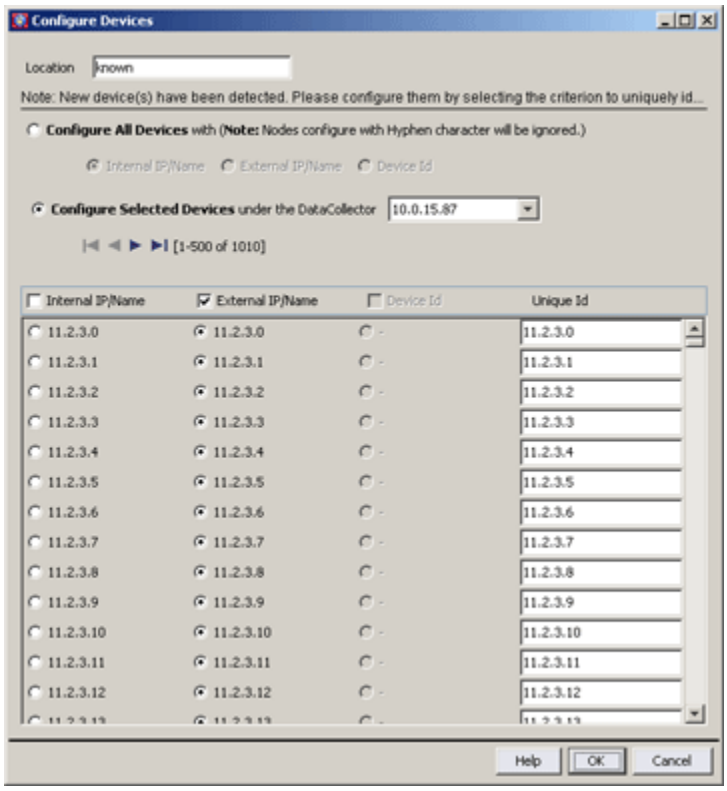
While using the trial license, all the devices are configured automatically. Under a permanent license, the Devices added from the add device wizard, appear under **Manually Added Device**. And the devices that are auto detected by the Device manager are displayed as **UnknownDeviceID**. These manually added and unknown devices can be configured from the **Configure Devices** screen.

If you want to configure all the devices at one go, you can use the **Configure All Devices** option and all the unconfigured devices are configured in one single attempt.

If you want to configure only selected devices, use the **Configure Selected Devices** option. When this option is selected, a maximum of 500 devices can be displayed in this window at one time. If the number of devices to be configured is more than 500 in number, you can navigate to the next page where the next set of to be configured devices are loaded and the user can perform batch configuration of syslog identified devices.

The Configure Devices screen lets you enter the Location Name where you want to associate all the devices.

Configure Devices



The Configure Devices screen displays information about the following:

1. **Internal IP/Name**: This column displays information about the Internal IP/Name of the added devices.
2. **External IP/Name**: This column displays information about the IP addresses of the added devices.
3. **Device Id**: This column displays information about the Device Id of the added devices.
4. **Unique Id**: In this column you can specify the Unique ID (UID). It can be from internal IP/external IP/device ID or can be any custom unique ID (UID) provided by the user.
   Note: Devices licensed hereafter would be uniquely recognized by this UID.
5. Select the any one of the above options or provide a UID based on which devices will be configured. Click **OK**.
6. All the manually added and unknown devices can now be licensed from the license manager or from the pop-up screen displaying the unlicensed devices.

Licensing Criteria

If the Device Manager identifies a new device ID in the log file, it adds the device ID under the Data Collector as UnknownDeviceId. And if you add a device using the Add Device Wizard it is displayed under **Manually Added Devices**.

To specify the licensing criteria for the newly associated devices click the **UnknownDeviceId**/**Manually Added Device** link, the **Licensing Criteria** dialog opens. Specify the criteria based on which this device must be licensed.

A device can be identified by any of the following identifiers:

- Internal IP/Name
- External IP/Name
- Device ID
- UID

Select any one of the identifiers and click **Save**. When you do this, you are prompted to license the device immediately, later, or never. If you select Now, The device immediately displayed as licensed on the Devices **screen**.

NOTE: The specified UID can be from internal IP/external IP/device ID or can be any unique ID (UID) provided by the user. Device licensed hereafter would be uniquely recognized by this UID.
- Double-click on the device from the Devices tab, if you need to change the UID at a later stage after configuring it. You can edit the UID of any primary device not more than five times.
- A device can be reported on only if it is licensed. Once the device is deleted the License can be reused for another device.

Change License and Change Policy Option

From the device manager tabs, i.e. Devices, NSA gives the option of changing a license and collection policy associated with a device. It greatly enhances the usability.

Change License:

When you right-click on the **License** column of a device, the **Change License** option is displayed. This option lets you change the trail license to a Permanent license.

NOTE: A license can be changed with a license of the same type or with a License of greater hierarchy.

Change Policy:

When you right-click on the Policy column of a device, the **Change Policy** option is displayed listing all the Collection Policies associated with the application. To assign a different collection policy, select a policy from the Policy Name list and click **OK**. Subsequently logs from the device are collected based on the settings defined in the policy.

NOTE: You can change the collection policy for the all the devices under a specific Data Collector by Right-clicking on the Policy column corresponding to the Data Collector row.

Collection Policies

NSA offers a visual interface to enforce collection policies.

Policy Manager

Threats and attacks span the entire network; therefore, it is imperative to collect real-time events of network activity across all IT components, 24 hours a day, seven times a week. The information security and event management, through real-time monitoring and concise reporting solely depends on the policies enforced for event data collection. NSA provides a comprehensive policy management module for event collection from devices.

NSA provides you with a visual interface to create and manage the policies for specific event data collection. You can create and enforce the event collection policies and policy templates for effective event management. The Policy Manager contains the following tab for policy creation:

- **Collection**: Use this tab to create and manage policies to collect event data from specific device (s).
-

IMPORTANT: Policies defined in the policy Manager are not applicable to ISA and AV devices.

Collection

The Collection tab on the Policy Manager displays the list of available collection policies. You can Add, Edit and Delete a collection policy from here. There are following factory made ready-to-use, collection policies available in NSA, they are:

- **No Collection**: This policy disables the collection of all the events from the devices and hence no data is available for monitoring or reporting if this policy is enforced.
- **Monitoring Only**: This Policy is meant to collect and stream events of Debug and higher severity levels for monitoring. It also appends raw logs of attack events, virus events and the severity events of debug and higher to the Delta.
- **Top Priority Events Only**: This Policy is meant to stream top priority events starting from warning to higher severity level for monitoring. The events of Debug and higher severity levels are collected. It also appends raw logs of attack events, virus events and the severity events of emergency and higher to the Delta.

Create Collection Policy

1. To create a new collection policy, click the **Add Policy** button from the Policy Manager. The Create Collection Policy window opens.
2. Enter a Policy Name.

3. Select a group/device under Data Collector/Device column and choose specific devices in that group on which you want to enforce the policy.
4. Click **Next**. On the next window, you can specify the event collection settings on events from following different sources:
    - Event Collection (Streaming Data)
5. Specify the event collection details and credentials. Click **Finish**, the Policy is populated in the Policy Manager.

Event Collection

In the Event Collection section, you can specify the severity of events to write into the delta files, specify the severity of events that are to be streamed to the monitoring console and the storing of the logs with respect to different activities occurring on the devices.

Collect Events of: Specify the lowest severity level of the events, events with this specified severity onwards to the highest severity level will be considered and saved in the deltas when the raw log files are compressed into delta files. To view all events or to write all events in the delta file, select Debug. Specify the events that should be considered, from the following drop-down list event severities list:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Information
- Debug

Monitoring: Check the monitoring box to enable streaming of log events for real-time monitoring. By default the Monitoring option is unchecked, i.e. the events are not considered for monitoring. To enable the streaming of events of selected severity onwards, to the Event Viewer select the severity level from the drop-down list. To view all events select **Debug**.

Append Raw Log in Delta: You can specify to append the native or raw logs to deltas till the selected severity level from the drop-down list. Other events that do not come under the selection will not be considered to be appended. You can specify to append the following types of events:

Severity: The available severity types are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice

- Information
- Debug

NOTE: Raw logs would be appended for only those devices that can stream their logs to NSA Data Collector.

Edit Collection Policy

Edit your selection of Group Name/Device and choose specific devices in that group on which you want to enforce the policy. Edit your preferences for collection policy as required and click **Save**.

Policy Synopsis

The factory made and the customized made Collection Policies are populated on the main Policy Name list-box. Follow the steps given below to view complete synopsis of a policy:

1. Select a policy name.
2. The complete synopsis of the policy settings is displayed on the right pane of the same window.
3. The complete details of the Event Collection and the events appended to the raw log data are shown in the same pane.
4. You can modify the selected policy by clicking on the **Edit** button.

Chapter 13: Policies

In simple words a Policy is a systematic set of statements to govern the upcoming decisions and actions of the user.

In NSA, a policy is a formal set of rules to define the course of action that the user needs to take under specific circumstances. A rule can dictate— which devices to consider, what event type to filter or negate, which entities with what values to add and so on. The user can associate a severity level to the Policy created. A policy is created on the customized device based rules or the existing rule templates. On implementation of a policy the user can choose to -- trigger an alert notification, or simply classify the Policy under an Event class by associating it to a report query. A user can add, edit, copy or delete a Policy.

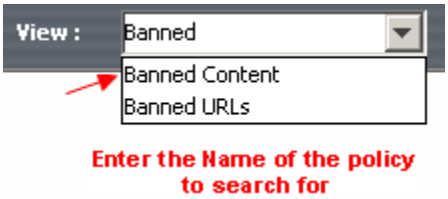
The main menu bar of the Policy window contains the following buttons: New Policy, Edit Policy, Copy Policy, Delete Policy and Rule Templates.

View: By default NSA installs with in-built policies. The number of default and customized policies put together can become difficult to track and manage. Therefore, the View drop-down list can help you display the policies classified based on the criteria on which they were defined. This helps you in filtering policies, which are Enabled/Disabled.

- All Policies
- Enabled Policies Only
- Disabled Policies Only
- Event Class Policies Only

Search through View:

In addition to restricting the view to display only those policies that conform to the selected criterion, you can perform a quick search to locate any particular policy by entering a search string.



For Example: If you want to locate a specific policy, enter its name in the View text box and the relevant Policy will be highlighted. As and when you create and save a Policy, the related details are listed on the main screen of this window. The following bottom line information is displayed in the columns:

1. Name of the Policy.
2. The description of the Policy as entered by the user while creating it.
3. The type of action to take on implementation of the Policy as prescribed by the user.
4. The Event Class details.
5. The Severity level associated with the Policy, as marked by the user while creating it.
6. The regular expression, depicting the Rule(s) and how they are associated with the Policy by using operators.

Add To Group

All the factory defined policies are placed under the **Default Group**. If the user wants to categorize the existing Polices or User Defined Polices under a new group, use the **Add To Group** option.

Follow the steps given below to add a policy to group:

1. Right-click on the policy that is to be added under a group.
2. All the existing groups in the Groups tab are displayed in the menu bar other than the default group.
3. Select the **Add to -> New Group** option if you want to create a new group or select an existing group to which you want to include the Policy.

Creating a New Policy

You can create a new policy from either Policies or Alerts. Basic difference between the policies created in these modules is with respect to the Mode of Action.

You can create policies on non-alert based actions like Event Class from Manage > Policies > New Policy Wizard.

What you can do on this window?

Create Event Class Policies - used to classify events matching certain criterion. All events generated within the Intranet or a DMZ can be classified as a separate class.

Basic Information

1. Click **New Policy** from the Policies main window, the **Create Policy** window opens.
2. Click New from the Manage > Policies main window, the Create Policy window opens.
3. Enter a Policy Name.
4. Select a group under which the policy should be placed from the **Policy Group** drop-down. By default, a new policy will be placed in the Default Group. To create custom group, click here for details.

5. Enter a short description of the Policy properties for future reference and the Impact of the Policy on the network once it is implemented and the proposed Remedy if it is a threat to the network security.
6. Define what mode of action to take on implementation of that Policy.
7. Select **Event Class** if you want to classify the events based on specific network areas (DMZ, internal or external networks), operating systems, IDS or IPS systems by grouping them under one Event Class. An Event Class represents one type of events used by NSA for alerting and reporting purposes.
    a. Select **Event Class**.
    b. Enter a unique Event Class name.
    c. Click the **Configure** button. The Configure window opens.
    d. Select the Threat level and furnish the threat level from the in-built list. The available options are:
        - Emergency
        - Alert
        - Critical
        - Error
        - Warning
        - Notice
        - Info
        - Debug
    e. Select the **Update Database for Selected Categories** option to save the matching events in the Database.
    f. Select the event categories that you want to send to the database. Press Ctrl and select the category (s) that you want to send to the database under the created Event Class.
    g. Click **Save** to save the Event Class, else **Close** the window.
8. Click **Next**.

NOTE:

- Selection of Database categories will increase database size because all the matched events will be saved in the database.
- By Configuring the Event Class on a Policy you can generate Reports, both complete and selective as defined in the Event Class settings.

Schedule Policy

In the new policy wizard from the schedule policy screen, you can specify the time during which the policy will be enabled.

1. If you want the policy to be enabled at all times, select the option '**This policy will be enabled 24 hours a day'**.
2. If you want the policy to be enabled only between the specified times, select the option '**This policy will be enabled during these times (use 24-hour time)**'.
3. Enter a Time Range by selecting the time from **From** and **To** drop-down time list and specify the time span within which you want to enable the Policy. Click **Add this time to schedule** button and the time range is populated in the Schedule box. You can add multiple Time Ranges to enable the Policy more than once in a day.
4. If you want to remove a time range, select the entry from the schedule box and click **Delete** button.

Set Rules

In the new policy wizard from the **Set Rules** screen, you can specify to create New Rule, Edit Rule, Copy Rule and Delete Rule. This window displays the list of Rules available for the Policy. Based on the requirement, each rule of the policy can either be enabled or disabled.

Basic Information

1. From the **Set Rules** screen, click **New Rule** button.
2. The New Rules Wizard opens. From here you can assign rules to a policy from two different sources, they are as follows:
    - Import from template
    - Select the '**Import From Templates**' option from the Basic Information screen of the New Rule wizard.
    - Select the Rule Template to import from the available custom made Rule Templates list. To import more than one templates press the Ctrl key and select the Rule templates.
    - Create New Rule
    - Select the **Create New Rule** option from the Basic Information screen of the New Rule wizard.
    - Select the Rule Template to import from the available custom made Rule Templates list. To import more than one templates press the Ctrl key and select the Rule templates.
3. If a template is selected, the Rule Name and Rule Description fields will acquire the details as available in the template.
4. If **Create New Rule** option is selected, enter an appropriate Rule Name and a short but apt description about the rule in the **Rule Description** box.
5. Click **Next**.

Identify Criteria

Create New Rule

- Device

Editing a Rule

1. Select the Rule that you want to edit from the Rule list populated on the Create Policy window. The column Base identifies whether the Rule is based on what criteria.
2. Click on the **Edit Rule** button from the Create Policy menu bar.
3. If you have selected a Device based rule to edit, the corresponding window opens. Similarly other edit rule window opens for the rule criteria you chose to edit.
4. The Rule name is non-editable.
5. You can edit the description of the Rule.
6. Make the necessary changes-- you can edit the settings on all the filters available in the list and also add new filters.
7. Click the **Next** button to proceed with editing process, else click the **Cancel** button to abort the task.
8. On the next screen if needed, you can change the way the operators are working on the sets of filters.
9. Click **Save** to save the edited Rule on the Create Policy window
10. Click **Save As Template** to save the edited rule as a template in the Rule Templates repository accessible from the Policies main window.
11. Click **Previous** to revert to the earlier screen to alter or recheck the filter settings.
12. Click **Cancel** to abort the task.

Making a Copy of the Rule

1. Select the Host Rule to make a copy of, from the Rule list populated on the Create Policy window. The column Base identifies whether the Rule is based on what criteria.
2. Click on the **Copy Rule** button from the Create Policy menu bar.
3. A copy of the selected rule is created.
4. The copy of the Rule is saved with a prefix "Copy_of_" followed by its original name.
5. You can edit the name and the description of the copy of the Rule.
6. You can edit any or all the filter settings followed by the operator settings pertaining to the original Rule and can also add new filters.
7. Click **Save** to save the Copy of the Rule on the Create Policy window.
8. Click **Save As Template** to save the Copy of the Rule as a template in the Rule Templates repository accessible from the Policies main window.
9. Click Previous to revert back to the earlier screen to alter or recheck the Device filters settings.
10. Click **Cancel** to abort the task.

Deleting a Rule

1. Select the Rule to delete from the Rule list populated on the Create Policy window.
2. Click the **Delete Rule** button from the Create Policy menu bar.
3. The dialog box prompts you for a confirmation. Click **Yes** to delete, **Cancel** to abort the task.
4. The Rule will be permanently deleted from the Policy.

Rule Expression

Once you create the Rule (s), you can combine/negate/select them and apply to a Policy by using the following operators:

1. **Negation**: Use this operator to negate or exclude a particular Rule and apply the rest to the Policy. The negated Rule appears prefixed with an exclamation symbol -"!" in the existing rules list.
2. **And**: Use the "And" operator to select and combine more than one Rule to apply in unison to the Policy.
    - Select a Rule from the existing rules list. For example —select RULE 1.
    - Select the complementary Rule from the existing rules list. For example—select RULE 2.
    - Click the "And" operator.
    - Click Finish.
    - The Operator settings appear in the Summary text box. In this case — (RULE1&&RULE2). Now both the rules are combined and will be executed in unison.
    - The "And" operator is denoted by an ampersand symbol (&&)
    - Click **Clear** to undo the Operator settings.
3. **Or**: Use the "Or" operator to select two Rules and apply one of them to the Policy.
    - Select a Rule from the existing rules list. For example - Select RULE 1.
    - Select the complementary Rule from the existing rules list. For example—select RULE 2.
    - Click the "Or" operator.
    - Click **Finish**.
    - The Operator settings appear in the Summary text box. In this case - (RULE1||RULE2). Now both the rules are combined and the one which meets the criteria first will be executed and the other stands void.
    - The "Or" operator is denoted by a pipe (vertical bar) symbol (||)
    - Click Clear to undo the Operator settings.
    - Press the Ctrl key and select more than one Rule at a time from the existing Rules list and click the operator you want to apply from the available operators except the negate filter. As the Negate operator works on one filter at a time.
    - By default the "Or" Operator is applied to the filter.
4. **Set Precedence**: Use Set Precedence to establish an order of importance to execute the rules. This will set the priority on the rules in a descending order. Follow the steps given below to set precedence on the Rules:

- Click on the Set Precedence button. A window displaying all the rules within the policy is opened. Select a Rule that is of utmost importance to be considered in the Policy. Let's say RULE 1 and then use move the rule into precedence list.
- Subsequently, after RULE1 if your want to consider RULE3 and RULE4, select RULE3, RULE4 from the existing rules and move the rules into precedence list.
- Next, Let's assume you set precedence on RULE2.
- The Set Precedence feature will establish an order of importance to execute these selected rules. The order is summarized in the Precedence Order text box. In this case the Precedence Order will appear as: RULE1, RULE3, RULE4, RULE2
- The importance associated is in a descending order: RULE1 > RULE3 > RULE4 > RULE2

NOTE: You can Set Precedence on the Rules even after applying the operators.

Choose Targets

1. The window displays licensed Nodes available with NSA application.
2. From the complete list of licensed nodes you can select:
    - If any of these nodes matches, then trigger the rule
    - Only trigger this rule if certain required nodes match
3. When option 2 is selected, click the **Correlate Nodes** button.
4. The **Set Correlation** window opens.
5. Enter a Correlation Threshold value to establish correlation between Audit Scores of the selected nodes.
6. Select the node (s) to correlate.
7. Click **Save** to save the correlation settings, else click **Cancel** to abort the task.
8. The Rule is now configured and is ready to apply on the Policy.
9. Click **Save Rule** button.

Set Permissions

Default Policies:

Admin Users: By default all in-built polices are accessible to all Admin User accounts of the application. Any logged in admin user can Edit the settings of the policy, Save the settings of the policy. It is up to this Admin User discretion whether to allow other NSA users to View this Policy and able to Edit or Delete this policy.

Power Users: The Power users have only Read-Only Permissions. Hence these policies are loaded to this user but cannot edit or modify anything.

User Defined Polices: If the user (admin or power users) creates a New Policy, then this user will automatically become the owner of the policy, this user can define access settings for other users using the permit other users using the Set User Permissions option present in the Create Policy window.

After creating a new policy, you can set the permissions for other NSA power users on this policy by clicking the Set User Permissions button. By default the User creating the policy will have All privileges on the Policy i.e., View, Edit and Delete.

For example: If a power user creates the policy, this user will have All the privileges for the Policy. From the Set User Permissions window this power user can define the Access Settings (permissions) for other NSA users on this policy. When a user with View privileges only tries to edit the Policy, following message is displayed.

When a user is Granted the privilege to Delete a Policy, automatically all other Access Settings are also granted as to Delete a policy, other access (View and Edit) should also be allowed for that user.

Summarizing the Permissions Scenario

User with:

- Read -> can view the policy settings as well as alert-archives
- Edit -> can change the filters (Read + Acknowledge + Clear)
- Delete -> can delete the policy (Read + Acknowledge + Clear + Edit + Delete)

Rule Templates

1. Click the **Load Rule from Templates** button from the Create Policy window.
2. The list of custom made Rule Templates available to load appears.
3. By default the there are nine Rule templates available in the NSA repository, which can be loaded on Policies. They are:
    - ipspoof attacks
    - URLsBanned
    - portrange
    - Allowed_Attacks_Viruses
    - Internal_Attacks_Viruses
    - VPN_Attacks_Viruses
    - InvalidPortAccess
    - Device Viruses
    - Blended Device Attacks
4. From the Policies and Alerts wizard you can also save custom policies and alerts as templates.
5. Select the Rule Template from the list that you want to load. To load more than one templates press the Ctrl key and select the Rule templates.
6. Click **Finish** to complete loading the rule template to the Policy or click **Close** to abort the task.

7. The Loaded Rule finally appears in the Create Policy window and is available to use in the Policy.

Editing a Policy

1. Select the Policy that you want to edit from the Policy list from the main Policies window.
2. Click on the **Edit Policy** button.
3. The Create Policy window opens.
4. The Policy name is non-editable.
5. You can edit the description of the Policy.
6. Make the necessary changes-- you can edit all the Rules created in the list and also load/delete rules from the templates.
7. You can change the way the operators are working on the sets of filters.
8. You can also edit the type of action to take on implementation of this Policy.
9. Edit the Event Class and the associated queries if needed.
10. Click **Save** to save the edited Policy.
11. Click **Previous** to revert back to the earlier screen to alter or recheck the filter settings.
12. Click **Cancel** to abort the task.

Making a Copy of the Policy

1. Select the Policy to make a copy of, from the Policy list on the main Policies window.
2. Click on the **Copy Policy** button from the main Policies menu bar.
3. The copy of the Policy is saved with a prefix "Copy_of_" followed by its original name in the main Policies window.
4. You can edit the name of the Copy of the Policy created.
5. You can edit the Rules and the settings of the Copy of Policy created.

Deleting a Policy

1. Select the Policy to delete from the main Policies window.
2. Click the **Delete Policy** button on the main menu bar.
3. The dialog box prompts you for a confirmation. Click **Yes** to delete, **Cancel** to abort the task.
4. The Policy is permanently deleted from the NSA.

Chapter 14: Identify Criteria – Policy & Alert Rules

Identify Rule Criteria for Agents

1. On the New Alert Policy wizard Set Rules, click **New Rule** button.
2. You can create a rule by importing any of the existing rule criteria templates or by defining new rule criteria for the agents. Select **Create New Rule** option.
3. Provide a Name and meaningful Description for uniquely identifying the rule. Click **Next**.
4. Select Agent from the **Category** drop-down list.
5. A comprehensive Agent Filter List is populated on the left hand side column of the Create Rule window based on your selection criteria. The list displays the following Agent filters:
    - Action
    - Current Size
    - Regular Expression Filters
      (Directory, File Name, Previous File Name, Registry Name, User Name)
    - USB Status
6. Select a Filter to apply to the rule.
7. Fill in all the details pertaining to the selected filter. The gist of the filter settings appear on the right hand corner box.
8. Click on the **Use Criteria** button to save the settings, or click **Delete Criteria** to cancel the filter settings.
9. If you want to negate the selected filter, select the **Negate Criteria** option.
10. Repeat the above steps to add more filters to the rule.
11. An executive summary of the filters created appears on a horizontal bottom box displaying the Filter names and their respective values.
12. Click the **Next** button to continue with the Filter settings or click **Cancel** to abort the task.
13. The Next screen displays all the created filters available to apply to the rule.
14. You can use the operators AND and Or to select the filters in combinations or to choose one of the selected two. Press Ctrl and select the filters and then specify the operator.
    The "And" operator is denoted by an ampersand symbol (&&) in the filter expressions.
    The "Or" operator is denoted by a vertical bar (pipe) symbol (||) in the expressions.
    By default the "Or" Operator is applied to the filter.
15. The Filter Expression summary is displayed in the bottom most horizontal box. The summary displays the way the operators are applied on the filters using the "&" and "|" symbols.

Note: The filter expressions on Rules can be as complex as you want them to be, in order to get down to the crux of the Rules.

---

16. Use the Negate expression to exclude the set filter expression on the rule. The negated filter expression is prefixed with an exclamation mark-"!".
17. Use the **Clear Expression** button to undo the operator settings on the filter expressions.

18. Click **Finish** to accept the Filter Expression.
19. Click the **Previous** button to revert back to the earlier page to add or modify filter settings.
20. Click **Create Template** to save the rule as a template to load in future policies.
21. Click **Next** button to define the target devices where this rule should be applied.

Applying Filters to a Rule

As described above there is an in-built list of filters available to apply on the rule. Let us consider each filter at a time and figure out how they can be applied to the Rule.

Action

1. Specify the Action Details to filter in the text box.
2. Click the **Use Criteria** button. The filter is added to the Filter list.
3. Click the **Delete Criteria** button to clear the settings.

Current Size

1. Select the criteria and enter the details of the size to filter in the text box.
2. Specify the current size value is Greater Than, Less Than or Equals To specified value.
3. Click the **Use Criteria** button. The filter is added to the Filter list.
4. Click the **Delete Criteria** button to clear the settings.

Regular Expression Filters

The following criteria can be defined as regular expression to apply on the rule.

- Directory
- File Name
- Previous File Name
- Registry Name
- User Name

1. Select any of the criteria and use the regular expression to consider for the selected criteria.
2. Click the **Use Criteria** button. The filter is added to the Filter list.
3. Click the **Delete Criteria** button to clear the settings.

USB Status

1. Specify the USB Status Details to filter in the text box.
2. Click the **Use Criteria** button. The filter is added to the Filter list.
3. Click the **Delete Criteria** button to clear the settings.

Creating a Device based Rule

1. On the New Policy wizard Set Rules, click **New Rule** button.
2. You can create a rule by importing any of the existing rule criteria templates or by defining a new rule criterion. Select **Create New Rule** option.
3. Provide a Name and meaningful Description for uniquely identifying the rule. Click **Next**.
4. Select **Device** from the **Category** drop-down list.
5. A comprehensive Device based Filter List is available on the left hand side column of the window. The list displays the following Device filters:
    - Action
    - Source IP
    - Destination IP
    - Destination Port
    - Protocol
    - Event Severity
    - Event Type
    - Event ID
    - Attack Type
    - Attack ID
    - Virus Type
    - Virus ID
    - URL
    - Rule
    - Content Category
    - Flow
    - Event Description
    - Attack Details
    - Shun
    - Spam Destination Email
    - Spam Source Email
    - Spam Type
6. Select a Filter to apply to the rule.
7. Select the Include Flow Data option if you want to filter the log data coming from the device through Flow stream along with the Syslog data. Flow data will not be considered if this option not selected.
8. If you want to negate the selected filter, select the Negation check box.
9. Fill in all the details pertaining to the selected filter. The gist of the filter settings appear on the right hand corner box.
10. Click on the **Save Filter** button to save the settings, or click **Delete Filter** to cancel the filter settings.
11. Repeat the above steps to add more filters to the rule.
12. An executive summary of the filters created appears on a horizontal bottom box displaying the Filter names and their respective values.
13. Click the **Next** button to continue with the Filter settings or click **Cancel** to abort the task.
14. The Next screen displays all the created filters available to apply to the rule.
15. You can use the operators "And" and "Or" to select the filters in combinations or to choose one of the selected two. Press Ctrl and select the filters and then specify the operator.
    - The "And" operator is denoted by an ampersand symbol (&&) in the filter expressions.
    - The "Or" operator is denoted by a vertical bar (pipe) symbol (||) in the expressions.
    - By default the "Or" Operator is applied to the filter.
16. The Filter Expression summary is displayed in the bottom most horizontal box. The summary displays the way the operators are applied on the filters using the "&" and "|" symbols.

NOTE: The filter expressions on Rules can be as complex as you want them to be, in order to get down to the crux of the Rules.

For Example: You can negate a Destination Port and a Destination IP Range or particular source IP. The filter expression in this case will be as follows:

!((Destination Port=[402,]&&Destination IP=[10.00.79.01-10.00.79.15,])||Source IP=[125.99.78.90,])

17. Use the Negate expression to exclude the set filter expression on the rule. The negated filter expression is prefixed with an exclamation mark-"!"
18. Use the **Clear** button to undo the operator settings on the filter expressions.
19. Click **Finish** to accept the Filter Expression.
20. Click the Previous button to revert back to the earlier page to add or modify the filter settings.
21. Click **Save** to save the rule under the newly created Rules.
22. Click **Save As Template** to save the rule as a template to load in future policies.

NOTE: The Rule created is in the disabled state, therefore it is imperative to enable it first from the Configure Rule option from the Create Policy window.

23. Click the **Cancel** button to abort the task.

Applying Filters to a Rule

As described above there is an in-built list of device filters available to apply on the rule. Let us consider each filter at a time and figure out how they can be applied to the Rule.

Action

1. Select either Allowed or Denied to filter events that are allowed or denied in a device/host.
2. Click the **Save Filter** button. The filter is added to the Filter list.
3. Click the **Delete Filter** button to clear the settings.

Source IP

1. Enter the **Source IP/Name** of the device you want to filter and report on only those events originating from the specified source.
2. To filter on events originating simultaneously from a series of devices, specify the IP Range by selecting the **Source IP Range** check box.
3. Select the option **Any** to consider all the source IP addresses.
4. Add the **Source IP/Name** by clicking the **Add** button.
5. Click the **Add/Edit** button. The filter is added to the Filter list.

Destination IP

1. Enter the **Destination IP/Name** of the device you want to filter and report on only those events having the specified Destination IP/Name.
2. To filter on events from a series of devices at a time, provide the IP Range by selecting the **Destination IP Range** check box.
3. Add the Destination IP/Name of the device or the range by clicking the **Add** button.
4. Select the option **Any** to consider all the destination IP addresses.
5. Click the **Add/Edit** button. The filter is added to the Filter list.

Destination Port

1. Enter the destination port number you want to filter for an event displayed in the **Event Viewer** console.
2. To filter on events from a series of devices at a time, provide the IP Range by selecting the **Destination Port Range** check box.
3. Click **Add**, and the port number you entered is added to the list.
4. Select the option **Any** to consider all the destination ports.
5. Click the **Add/Edit** button. The filter is added to the Filter list.

Protocols

1. Select the protocols you want to filter and click  to move them into the Selected Protocols list. You can also add new protocols.
2. You can add a new protocol by clicking the Add button.
3. Click the **Add/Edit** button. The filter is added to the Filter list.

Events Severity

1. Select the Event Severity from the following list:
   - Emergency
   - Alert
   - Critical
   - Error
   - Warning
   - Notice
   - Information
   - Debug
2. Select the protocols you want to filter and click  to move them into the Selected Protocols list.
3. You can also add a new severity by clicking the **Add** button.
4. Click the **Add/Edit** button. The filter is added to the Filter list.

Events Type

1. Select the Event Types from the following list:
   - TRAFFIC
   - IPSEC
   - DROP
   - BLOCKED
   - IDS
   - VPN
   - SYSTEM

2. Select the event types you want to filter and click  to move them into the selected event type list.
3. You can also add a new event type by clicking the **Add** button.
4. Click the **Add/Edit** button. The filter is added to the Filter list.

Event ID

1. Select the Event IDs from the available list.
2. Select the event IDs you want to filter and click  to move them into the selected ID list.
3. You can also add a new event ID by clicking the **Add** button.
4. Click the **Add/Edit** button. The filter is added to the Filter list.

Attack Type

1. Select the Attack Types from the available list.
2. Select the attack type you want to filter and click  to move them into the selected attack type list.
3. You can also add a new attack type by clicking the **Add** button.
4. Click the **Add/Edit** button. The filter is added to the Filter list.

Attack ID

1. Select the Attack IDs from the available list.
2. Select the attack IDs you want to filter and click  to move them into the selected attack ID list.
3. You can also add a new attack ID by clicking the **Add** button.
4. Click the **Add/Edit** button. The filter is added to the Filter list.

Virus Type

1. Select the Virus Types from the available list.
2. Select the virus types you want to filter and click  to move them into the selected virus type list.
3. You can also add a new virus type by clicking the **Add** button.
4. Click the **Add/Edit** button. The filter is added to the Filter list.

Virus ID

1. Select the Virus IDs from the available list.
2. Select the virus IDs you want to filter and click  to move them into the selected virus ID list.
3. You can also add a new virus ID by clicking the **Add** button.
4. Click the **Add/Edit** button. The filter is added to the Filter list.

URL

1. Select the URLs from the available list.
2. Select the URLs you want to filter and click  to move them into the selected URL's list.
3. You can also add a new URL by clicking the **Add** button.
4. Click the **Add/Edit** button. The filter is added to the Filter list.

Rule

1. Select the rules from the Available list.
2. Select the rules you want to filter and click  to move them into the selected rule list.
3. You can also add a new rule by clicking the **Add** button.
4. Click the **Add/Edit** button. The filter is added to the Filter list.

Content Category

1. Select the Content Categories from the available list.
2. Select the content categories you want to filter and click  to move them into the selected content category list.
3. You can also add a new content category by clicking the **Add** button.
4. Click the **Add/Edit** button. The filter is added to the Filter list.

Flow

1. Select either Allowed or Denied to filter events that are allowed or denied in a device.
2. Click the **Add/Edit** button. The filter is added to the Filter list.

TIP: Set your device interfaces correctly from the Devices/Groups user interface for this filter to work properly.

Event Description

1. Enter the event description you want to filter in the Event Description box. You can also use wild card '*' to filter any specific word or sentence in the description.
2. Click **Add/Edit Filter** button. The filter is added to the Filter list.

Attack Details

1. Enter the details of the attack to filter in the Attack Details box. You can also use wild card '*' to filter any common string in the description.
2. Click the **Save Filter** button. The filter is added to the Filter list.
3. Click the **Delete Filter** button to clear the settings.

Shun

1. Select Yes to filter shun events or No to ignore shun events occurring on the device(s).
2. Click the **Save Filter** button. The filter is added to the Filter list.

3. Click the **Delete Filter** button to clear the settings.

Spam Destination Email

1. Enter the email address of the Spam Destination in the Spam Destination Email text box. You can also use wild card '*' to filter any common string.
2. Click the **Save Filter** button. The filter is added to the Filter list.
3. Click the **Delete Filter** button to clear the settings.

Spam Source Email

1. Enter the email address of the Spam Source in the Spam source Email text box. You can also use wild card '*' to filter any common string.
2. Click the **Save Filter** button. The filter is added to the Filter list.
3. Click the **Delete Filter** button to clear the settings.

Spam Type

1. Select the Spam Types from the available list.
2. Select the Spam types to filter from the available entities list and click  to move them into the selected entities list.
3. Click the **Save Filter** button. The filter is added to the Filter list.
4. Click the **Delete Filter** button to clear the settings.

Configuring a Device based Rule

The Rule is created in a disabled state therefore you ought to enable it first in order to apply it to the Policy.

1. The window displays the name of the Device Rule along with all the Devices licensed to the NSA application.
2. From the complete list of licensed Devices select a Device(s) to configure the rule on.
3. Set a threshold value on the Rule.
4. Set the Refresh interval by selecting a value from the drop-down list.
5. Select Correlation to establish correlation between the selected Device(s).
6. Click **Set Correlation** button, the Set Correlation window opens.
7. Select the Devices(s) to correlate to the Device selected on the previous window.
8. Enter a Correlation Threshold value.
9. Click **Save** to save the correlation settings, else click **Cancel** to abort the task.
10. The Created Device Rule is now configured and is ready to apply on the Policy.

Alert Delivery

When an alert is generated, you can view it straight away on the Alert Manager by leaving the Alert Notification check box clear in the Configure Alert window or alternatively have it delivered by using any one or both the ways of notification, they are:

- E-mail
- SNMP Trap

E-mail Notification

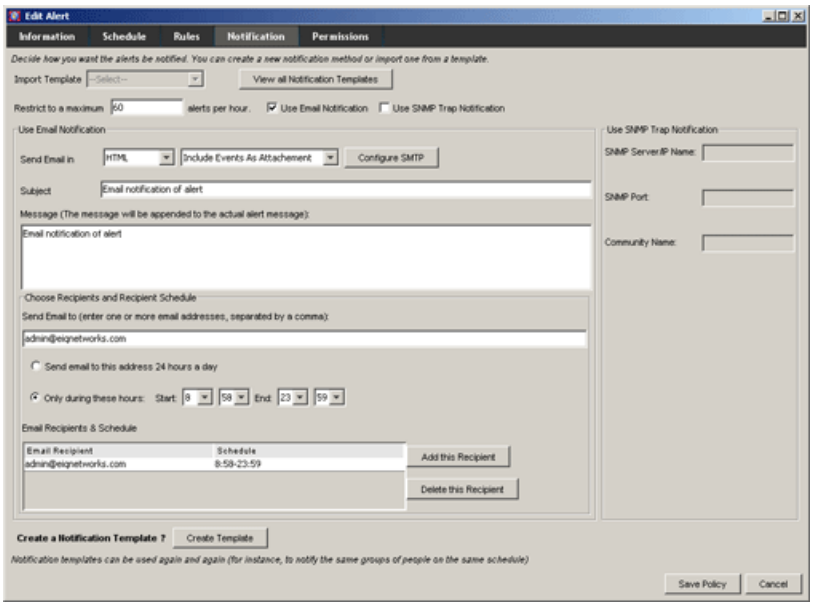
Select the E-mail check box for receiving alerts via e-mail. You can choose to not to include events in the generated alert. Also you can select to include events in the body of the e-mail or as an attachment. The alert details will be attached as an HTML file.

Select any one of the options given below:

- Do Not Include Events
- Include Events In Body
- Include Events as Attachment

Leave the check box clear and the alerts notified through e-mail will contain only the time, alert name, alert description, and a message.

The Alert Delivery Screen



NOTE: An alert message can be configured to be sent in either HTML or Text format.

E-mail Details

You can set the time period with in which if an alert is generated, it should be notified to a specific e-mail address.

Follow the steps described below to add an e-mail recipient:

1. Enter the time **From** to time **To** in the hh:mm format and the recipient's e-mail address. If an alert is generated within the specified time bounds, the alert message will be sent to the specified recipient.
2. Click the **Add** button. The e-mail ID is added to the recipient list.
3. Enter the subject and the message that should appended to the alert notification.
4. Enter the threshold figure for the number of e-mails that you want to receive in an hour. For receiving e-mails first configure the SMTP server.
5. To configure the SMTP server, click the **Configure SMTP** button which will take you to the Mail Preferences dialog box in the Options tab.
6. Specify the SMTP (Simple Mail Transfer Protocol) mail server name and user ID for NSA to send an e-mail alert whenever a specified event type or attack activity is detected or if the total number of attack attempts exceeds a specified value.
7. Finally, click **Save**.

Templates

NSA gives an option to create Alert Delivery templates, which can be used to notify intended recipients (admin users) for triggered alerts. You can directly import the settings defined in a template to any other Alert Delivery settings.

The Templates window displays the list of existing Alert Delivery templates on the Left pane and the corresponding synopsis for the template on the Right pane.

SNMP Trap

SNMP (Simple Network Management Protocol) allows you to instantiate a trap-directed alert notification called the SNMP Trap. Trap-directed notification can help you save network and agent resources by eliminating the need for SNMP requests, and through minimized SNMP polling.

To configure NSA to send traps to the SNMP server, follow the steps described below:

1. Select the **SNMP Trap** check box
2. Enter the appropriate details of the SNMP server **IP / Name**, **SNMP Port**, and **Community Name**.

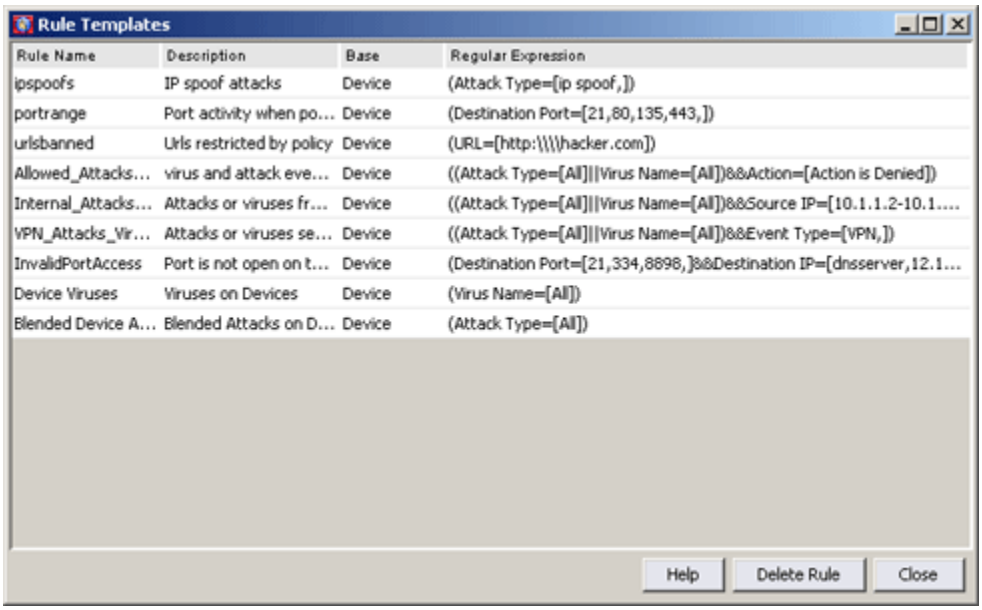
The idea behind trap-directed notification is as follows: if a large number of devices are configured to send alerts, and each device has a large number of objects, it is impractical to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the Alert Manager without solicitation. It does this by sending a message known as a trap. After receiving the event, the Alert Manager may choose to take an action based on the threshold set for the event.

Rule Template

A Policy is based on Rules. You can create and save Rules as templates in one common repository. Every time you want to apply a Rule to the Policy you can select from the pre-formatted Rule templates. The Rule Templates can be applied in combinations, across all the policies.

Creating Rule Templates

1. On the main Policies window, click Rule Templates button.
2. The Rule Template window opens.
3. From here you can either select the preformatted templates or create new templates.
4. Click on the **New Template** button and the Create Rule window opens where you can create templates based on:
    - Device



Editing a Template

1. Select the Rule template that you want to edit from the Rule template list from the Rule Templates window.
2. Click on the **Edit Template** button.
3. If you have selected a Device based rule to edit, the corresponding device window opens.
4. The Rule name is non-editable.
5. You can edit the description of the Rule.
6. Make the necessary changes-- you can edit the settings on all the filters available in the list and also add new filters.
7. Click the **Next** button to proceed with editing process, else click the **Cancel** button to abort the task.

8. On the next screen if needed, you can change the way the operators work on the sets of filters.
9. Click **Save** to save the edited Rule Template.
10. Click **Previous** to revert back to the earlier screen to alter or recheck the filter settings.
11. Click **Cancel** to abort the task.

Delete a Rule Template

1. Select the Rule template to delete from the list on the Rule Template window.
2. Click the **Delete Rule** button.
3. The dialog box prompts you for a confirmation. Click **Yes** to delete, **Cancel** to abort the task.
4. The Rule Template will be permanently deleted from the repository.

Set Threat Levels

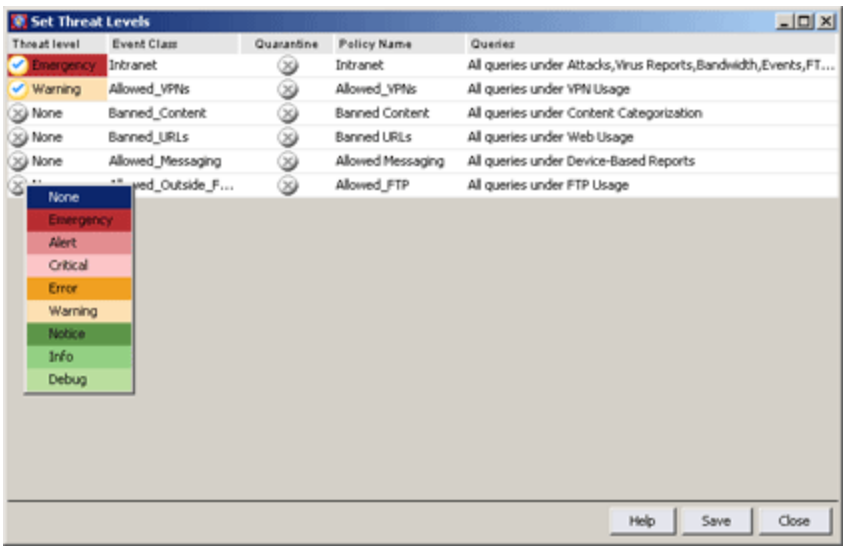
A potential adverse event which is malicious by nature or is incidental and that can put the network and system assets at stake can be classified as a threat to the network security of an enterprise.

Event Logs from vendor specific devices come with pre-assigned severity levels for each event depending upon the potential or incidental degree of associated threat. Each severity level is depicted in a different color, which is vendor specific.

There are eight Threat levels, each identified by a corresponding color. From lowest to highest, the levels and colors are:

- Debug = Violet
- Info = Cyan
- Notice = Green
- Warning = Orange
- Error = Yellow
- Critical = Blue
- Alert = Pink
- Emergency = Red

Now, NSA gives the flexibility to the Super Admin User to change the threat level associated with a class of events and set it according to his perception of the threat. For example, if the severity level of an Event Class is ‘Emergency’ and is depicted in red in the vendor logs, but the administrator does not consider them as high level threat events, he/she can use the Set Threat Level option and change the threat from ‘Emergency’ to say ‘Warning’. Henceforth the severity of events which belong to this Event Class will be marked as Warning and will be depicted in orange. The altered threat level is updated in Event Viewer for real-time monitoring and is also reflected in all graph types and reports.



Changing threat levels

1. Select the Event Class on which you want to change the threat level.
2. Click on the select Threat Level icon to select any of the threat level which you want to apply to an event class.
3. Click **Save**.

Chapter 15: Profiles

A profile is a set of instructions identifying the locations of your device logs, how data must be accessed, the method followed to analyze data, how IP addresses must be resolved, and customization of reports. Profiles also facilitate you to choose filters that help you narrow down your data to the information you need most, which can save time and resources. Profiles can be created using the New Profile wizard. When the wizard completes, the profile appears in the profile list.

The Profile Manager main window contains the New Profile, Edit Profile, Copy Profile, Delete Profile buttons.

Creating a New Profile

A profile is a group of settings configured to complete a specific task. Once configured, you can use it repeatedly to generate reports whenever necessary. You can also edit or delete a profile as necessary. The first step towards creating a new profile is to assign a unique name. To do this, carry out the following steps.

To create a profile, follow these steps:

1. On the main Profile Manager window, click **New**. The New Profile wizard opens.
2. Type in a name in the **Profile Name** text box.
3. Select from the following sources; the input for the profile to be created:
    - Select NSA Database if the NSA Data Collector has been configured to collect log file data and store it in the built-in database. OR
    - Select File to migrate log file data to the database and generate a report.
4. Specify the Date Range to configure the Profile to consider data of only the specified dates.
5. Select the devices you want to report on. Click **Next**.
6. The DNS Lookup screen opens. Select a resolution option and click **Next**.
7. Add the filter template you want to apply and click **Next**. To use a pre-defined report, select a report from the list. To create a custom report, click New Report and supply the required details and click **Next**. The Report Style window opens. Click here for details.
8. Select the report format, the template, the table format (for HTML reports only), the language, the organization name and the logo file to use and click **Next**. The Save Report screen opens. Click here for details.
9. To e-mail your report, select the **Mail To** check box and specify the recipient addresses in the text box. To upload your report to a remote site, select the FTP check box, specify host name, user name, and password and click **Finish**.

NOTE(S):

- NSA supports McAfee Intrushield logs collected by the Data Collector and not from the Log File as source option.
- Creating File based profiles on a Central Server is possible only when it has at least one Data Collector configured/reporting to it.
- A Power user cannot create profiles based on File option.
- Once a profile is created, the Profile Name and the log source (NSA Data Collector/File) cannot be edited.
- Use of wildcards is not supported in the FTP retrieval path.
- NSA receives log data once every 30 minutes (from the NSA Data Collector) and the database is updated once every hour. So a user cannot generate any report within the first hour.
- Use the File option instead of NSA Data Collector to generate reports. In this case, the report is generated immediately.

NSA Data Collector as Source Input

Select this option if NSA Data Collector is collecting the log data from the Devices.

File as Source Input

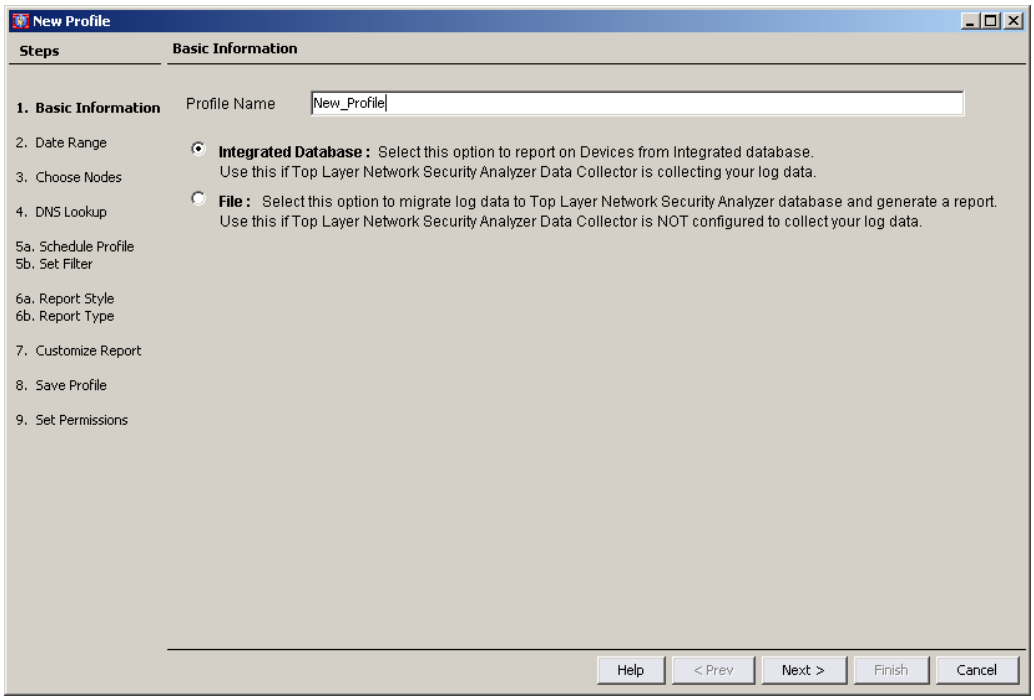
Log File Source: A file which would be the source can reside on the local machine where NSA is installed or on a FTP site. Select the File or FTP option based on the location of the log file.

Parse Archive Generated By MARS: Select this option if you want to parse log archive present in the shared location of the Cisco MARS device.

Device Identifier: Select this option to identify, license and further generate a report on the data present in the log file which is henceforth represented with the string provided in the Device Identifier text box.

Generate Report after Parsing the Log Data: Select this option if you want to parse the log file and subsequently generate a report immediately.

Leave the check box clear if you want the data present in the log file only to be parsed. The report on this profile can be generated only after the next aggregation cycle.



Generic File Names

NSA provides a generic method for specifying input and output file names in the profile. You can enter generic file names directly in name text box or you can use the Grammar Syntax feature to specify input and output file names. This feature is useful in scheduling repetitive tasks for which the log file name is structured on a timestamp format.

File Specification Grammar Macros

File Specification Grammar Macros		
Macro (Code)	Description	Format
%b%	Abbreviated month name	(Jan-Dec)
%B%	Full month name	(January-December)
%m%	Month	(01 – 12)
%d%	Day of month	(01 – 31)
%H%	Hour in 24-hour format	(00 – 23)
%y%	Year without century	(00..99)

%Y%	Year with century	(2000-2099)

NSA allows you to use wild card specification in the file name specification, and understands standard DOS directory wild cards (i.e., *). You can specify the relative day, week, month or year by decreasing or increasing the specific value. The same syntax is used to specify file names for output reports.

Grammar Syntax Examples

Generic Naming – Grammar Syntax Examples		
File Name Specification	Sample File Name+	Represents
eIQ%m%%d%%y%.log	eIQ062008.log	June 20, 2008
eIQ%m%%d%%Y%.log	eIQ06202008.log	June 20, 2008
eIQ%Y%%d%%B%.log	eIQ200820June.log	June 20, 2008
+ Assuming current date is November 02, 2009.		

To specify file names using the Grammar syntax, follow the steps below:

1. Click New Profile and select File to migrate log file data to the NSA database and generate a report. Click **Next**.
2. Click **Grammar** to display the Grammar screen.
3. Click **Browse** and go to the location where generic log files are stored.
4. Select the timestamp format for the generically named files. Based on the log file naming convention of your log file, select the appropriate date format from the Date Format drop down list. You can add an alphabetical prefix to the format and select from different file extensions in the suffix box.
5. In the Add/Subtract text box (Year, Month, and Day/Weeks) specify the time stamped log file that you want to use as the input. For example, to attach to yesterday's log file, enter –1 in the Day text box with respect to the current system date.

Selecting Accessible Nodes or Groups

From this screen, you can select all the accessible groups, nodes a user has permissions to report on. User can also select specific nodes of choice from the available list of all licensed nodes. User can also specify the DNS Lookup settings for the reports.

If your network environment is configured such that more than one device/host write log data into a single log file, this screen will allow you to select only the devices you wish to report on and filter out data from the remaining.

Follow the steps described below to select the devices you want to report on from amongst the licensed network devices:

1. On the Node Settings screen, select All Accessible Nodes option to generate the report on all licensed nodes configured to NSA.
2. Select **Accessible Groups** option if you want to generate your report based on the logical grouping of nodes.
3. If you want select specific nodes, you can use the **Select Custom Nodes** option. From the **Choose** button, select the devices as per the requirements. Click **OK**.
4. Click **Next**.

DNS Lookup

NSA can resolve the IP address, as found in the collected device log data, into meaningful host names using Domain Name System (DNS) resolution. Each Internet address can be resolved (if defined in the DNS of the owner of the IP number) into a domain name, which is easier to remember and makes the NSA reports more readable. Should the domain name not be defined for a specific IP address, the resolution will fail and only return the IP number to NSA, which is displayed in the report.

It is a good idea to increase the size of the DNS cache that is built into NSA should the number of unique IP numbers grow. Select the size of cache file from the drop-down list in the New/Edit Profile > DNS Lookup tab if you want NSA to consider previously resolved IP addresses stored in the cache. An important consideration is that if a cache is very large and never reaches the point of being filled, very old lookup information may be used in the reports.

The working order for DNS lookup in NSA ….

- Is the IP number defined as an intranet address?
- If not, check the DNS cache if it has been resolved earlier and is still stored.
- If not found in the DNS cache, the lookup will then call the DNS for resolution.

The lookup of IP numbers is based on all of the IP numbers that will be visible in report tables, should a report table contains 100 IP numbers, and these are the ones that will be resolved.

Components on the DNS Lookup Screen

- **Do not resolve IP addresses**: Select this button if you do not want to resolve numeric IP addresses into host names. This will speed up the processing of log files. By default, this option is selected.
- **Resolve the unresolved IP addresses into fully qualified host names**: Select this button if you want to resolve numeric IP addresses into domain names.
- **Perform resolution of IP addresses into host names using cache**: Select this button if you want to perform resolution i.e., from domain names to IP addresses and IP addresses to domain names using cache. Click **Next**.

Filter Templates

Profiles look at the results based on the filters you have defined, and ignore everything else. If you want to filter specific information, add a filter template according to your requirement. You cannot use more than one filter template for a profile. You can create, manage and use filter "templates" that can be used across your profiles.

To define a new filter template click on the **Add** button, his will direct you to the **Filter Template** screen, where new filter templates can be created.

You can choose to apply only one filter template on a profile. From the list of available filter templates, select the filter template you want to apply on the created profile.

NOTE: Make sure that the selected filter template contains all the filter definitions you want to apply on the profile.

Click **Next**.

Creating a New Filter Template

NSA provides complex, multi-level filters to sift data to analyze and present in reports. These filters let you focus on only the data you need and ignore the rest. For instance, if you want to generate a report on how many visits a particular group of IPs made to your website between two given dates, you can create a filter that limits your report to the IPs for the dates of interest.

This section provides you the information on how to create and set up filter templates for Profiles.

1. Type a descriptive name in the **Template Name** text box. Make sure this name is easy to remember and descriptive of the data you are trying to filter.
2. Select the Filter from the available list of filters.
3. Select the Include filter button if you want to include the data pertaining to this filter.

4. Select the Exclude filter button if you want to Exclude this filter data pertaining to this filter
5. Furnish the required details for the filter settings, Click **Add**.
6. Click **Save Filter**. The filter created is listed below along with its respective value. Click **Delete Filter** to clear the filter setting.
7. Set all the filters that you want to assign to the Template.
8. Click **Save** to save the Filter Template, else Click **Cancel** to abort the task.

Filter Elements

The following table provides information on each of the filter elements that can be used to create a filter:

Filter Name	Column ID	Description
Action	act	events/attacks (Device) Has only two values (allow, deny)
Category	cat	Device Category filter
Source	cli	Device Client (Source) filter
Description	desc	Description filter
Direction	dir	Bound filter for device (Has two values - In, Out)
Destination	dst	Device Destination filter
To	dstemail	Destination email (To) filter for Firewall Devices
Event Code	ec	Event Code Filter
Extension	ext	Extension filter (Device Virus)
Protocol Family	family	Protocol Family filter (Device)
Gateway	gw	GateWay filter (VPN)
Hour	hod	Hour of Day filter
Port	port	Port filter
Protocol	pr	Protocol filter
Severity	pri	Severity filter for Device(Emergency(0) - Debug(7))
Request	req	Request filter
Rule	rule	Rule filter (Device)
Description	shortdesc	Short Description filter
Site	site	Site Filter (Web)
From	srcemail	Source Email (From) filter (Device)
User Name	user	User Filter (User Name)
Virus Category	vcat	Virus Category filter (Device)
Virus Name	virus	Virus Name Filter

Scheduler

The Scheduler provides a visual interface to schedule reporting. You can schedule to run profiles automatically at specific date and times, which is particularly advantageous when you are running reports at regular intervals. Using the Scheduler, you can schedule tasks to run on specific dates and at specific times.

Scheduling a Profile

In the new profile wizard, the Scheduler screen opens. The list box contains all the scheduled tasks. Click the **Add** button to schedule a new task or select an existing task to edit.

Add Task

To schedule a task for a profile to generate reports at regular intervals, create a task using the Add Task wizard.

1. Click **Add**. The **Add Task** wizard opens.
2. Enter a name in the **Task Name** box.
3. Select the frequency of the task, i.e., how frequently you want the task to be executed.
4. Click **Next**.

NOTE: Only those profiles created by selecting the NSA Data Collector or File with grammar settings can be scheduled.

Scheduling Task by Hour

To schedule the task on an hourly basis select the Hour button and specify the interval.

1. The **Start Time** indicates the time at which you want the scheduled task to start. The current time is displayed in the hh:mm:ss by default. To change it, just specify a different time value. For example, 13:49:37.
2. The **Start Date** indicates the day you want the scheduled task to start. Use the **Calendar** button to select the start date or enter a date in the mm/dd/yyyy format.
3. The **After Every** indicates the interval at which you want the scheduled task to start. The intervals are 1, 3, 6, and 12 hours.
4. Click **Finish**.

Scheduling Task by Day

To schedule the task on a daily basis, select the Daily button and specify the time. You can also choose to have your tasks performed either every day or on weekdays only. Follow the steps described below to schedule a task by day:

1. Select the **Everyday** button to schedule the daily task and click **Next**.
2. Enter the start time to indicate the time at which you want the scheduled task to start. For example, 18:24:30,
3. The **Start Date** indicates the day you want the scheduled task to start. Use the calendar to select the start date, or type in a date.
4. Click **Finish** to save your settings.

Scheduling Task by Week

Select the Weekly button and click **Next** to bring up a dialog box where you can select the days of the week and the start time. This will result in the scheduled job being performed on the selected days of the week. The start time is specified in the Start Time edit box. The scheduled reports will not be generated before this time. Enter the time at which you want the scheduler to begin scheduling your tasks.

Follow the steps described below to schedule a weekly task:

1. Select the **Weekly** button to schedule a weekly task and click **Next**.
2. Enter the start time to indicate the time at which you want the scheduled task to start. For example, 18:24:30.
3. The **Start Date** indicates the day you want the scheduled task to start. Use the calendar to select the start date.
4. Select the days of the week on which you want to run the tasks.
5. Click **Finish** to save your settings.

Scheduling Task by Month

Select the Monthly button and click **Next** to bring up a dialog box where you can select the month, start date, and the day of each month when you want to generate the report. You can also generate the report of a specific day of the week of each month.

Follow the steps described below to schedule a monthly task:

1. Enter the **Start Time** to indicate the time when you want the task to start.
2. Enter the **Start Date** to indicate the date on which you want the task to start.
3. Click the **Day** button to choose the day of the selected months on which you want the task to run or the **Every** button to choose the day of the week of the selected months on which you want the task to run.
4. Select the months of the year when you want the task to run and click **Finish**.

Scheduling One-Time Tasks

Select One Time Only button and click Next to bring up a dialog box where you can select the start time and start date when you want to generate the report.

Follow the steps described below to create a one-time task:

1. The **Start Time** indicates the time when you want the scheduled task to run.
2. The **Start Date** indicates the day you want the scheduled task to start. Use the calendar push button to specify the start date or enter a date.
3. Click **Finish** to save your settings.

Report Type

You can generate a report either for a single device or for all the devices using the NSA.

- A single combined report for all selected devices.
- Individual reports for each selected device
- Group based report
- Interface-based report

Single combined report: You can generate a single combined report for all the devices that you have selected in the profile by using this Report Type.

Individual reports for each device: You can generate an individual report for each device that you selected in the profile. Using this option, you can obtain the list of events and individually monitor the occurrence of events on each device and scrutinize the performance of each device and set thresholds specific to devices.

The individual reports are:

- Generated/stored in separate folders under the Profile. The folder name will be the device IP or host name.
- The report name will have the suffix '_IP or host name' of the device.

Group based report: Using this option, you can generate a report for the entire group just by creating a profile with the group selected.

Interface based report: Using this option, you can enable reporting only on interfaces and devices and not virtual devices.

NOTE: If you select your report to be a combination of options other than single combined report, only one report is displayed in the report view and all the reports for other devices are stored in a user-specified location.

Query By

Use the Query By option to generate reports classified By Device/Host, By Group, By Day or By Event Class.

Device: Select this option to generate a report with an additional column which gives the details of the selected Devices.

Group: Select this option to generate a report to query on the Group to which the selected device/host belongs. For example, if you select two different devices present in more than one group then the report is generated with an additional column-- Group. This appended column gives the Group details of the selected devices. This query is particularly useful when the administrator assigns privileges for the Non-admin users to access only a few Devices configured on the application.

Day: Select this option to generate a report to query on the Day. This report appends a column-Day that gives the details of the day when that particular data came about.

Event Class: Select this option to generate a report to query on the Event Class. The drop down box lists the event classes created in policies module, Select the event class on which you want to query and generate a report.

NOTE: You can query by the above options in the reports from the security center also.

Trends: Selecting this option will append the following columns in the report, which will help you to judge the event trend:

- Today's Count
- Yesterday's Count
- Last Seven Days
- Current Month

Use this option to record the trend of specific current and previous events happening at the devices. This helps in determining the number of times a particular event type occurred over a period of time.

Report Style

You can customize the look and feel of reports as per your choice by selecting from 11 different templates and 10 table formats. You can also choose from HTML, MHTML, MS Word, MS Excel, PDF, and Text reports formats.

- **Format** — Includes HTML, MHTML, Microsoft Word, Microsoft Excel, PDF, and generic text file formats into which the content of the report will be generated.
  Internet browser settings for opening different formats of Reports after you generate them:
  PDF reports: Go to Internet Options > Advanced Settings > Security and leave the check box Do not save encrypted pages to disk clear for the PDF reports to open upon generating them.
  MS-Word and Excel reports: Go to Internet Options > Security > Security Settings. Click on the Custom Level Button and Enable the "Automatic prompting for File Downloads" under Downloads.

NOTE: MS-Office must be installed before you try to generate reports in WORD or EXCEL formats. Also Adobe Reader 6.0 and above to view the reports in PDF format

- **Template** — You can determine the basic structure of the report. The drop-down box allows you to select from a number of pre-configured report styles that have different fonts and colors. They are Cool, Vintage, Cascade, Serene Arcade, Sand Ribbon, Wise Monk, Capri Blue, Glass Block, Trendy, Standard, and Orange Spice. A Template is applicable for generating reports in HTML and MHTML formats only.
- **Table Format** — Select the format of the tables used to present tabular data in Microsoft Word reports. The table formats are Simple,

Colorful, Columns, Grid, Classic Grid, List, Classic List, Contemporary, Elegant, and Professional.

- **Organization** — This field allows you to select the company name as it will appear in reports. Typically, this field is used to present the name of the company creating the report.
- **Logo File** — The Logo text field is where the user can specify the logo file that will be displayed in reports. The default logo is the logo.gif and is picked from the folder [Installation Directory]\xhtmlfiles\logo.gif. To display your company logo, replace this image with your logo in this folder, or specify the absolute path to your logo file is in a different location. For example if your logo file is mylogo.gif and is in a folder named "images" in drive D: then the absolute path to the file would be D:\images\mylogo.gif.

NOTE: To open MHTML report in a Firefox/Mozilla browser, download and install the IE Tab add-on/extension from the following location: https://addons.mozilla.org/firefox/1419/

Specifying Report Styles

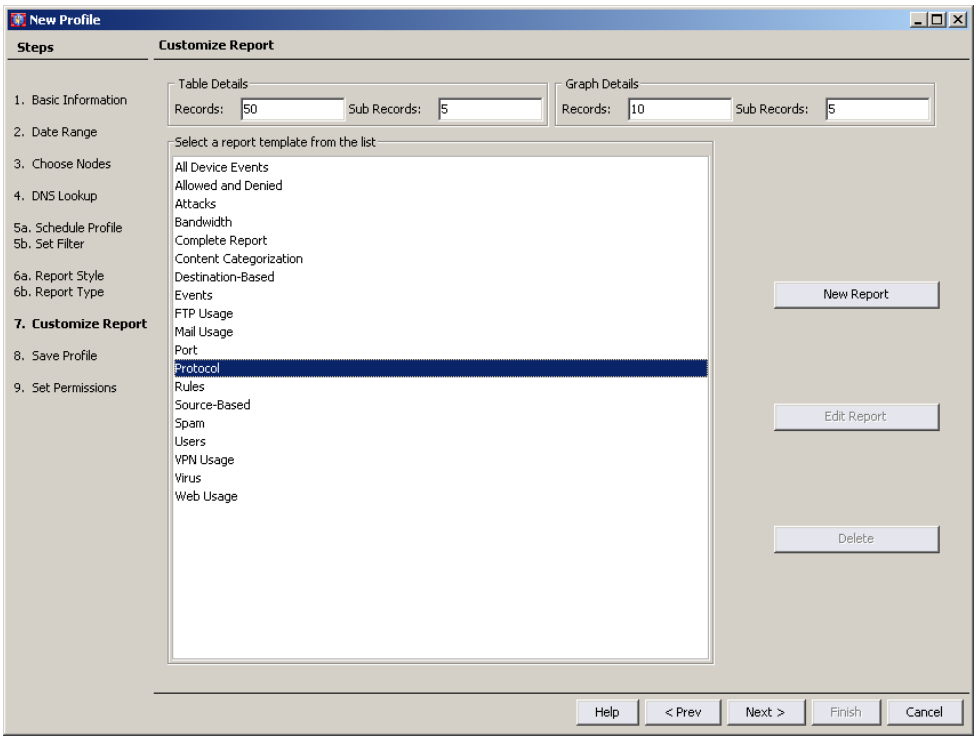
To specify the format of reports, follow these steps:

1. In the reports style dialog, click on the **Create Template** button. The new template window opens.
2. Enter the template name. Click  to select the background and query font colors.
3. Click **Save**.

Customizing Reports

NSA offers the flexibility to customize the reports by selecting a report title from the comprehensive in-built list. You can generate customized reports on Devices by selecting the respective report title.

The Report Customization Screen



A custom report is a report that you can create by including only the selected queries that meet your specific requirements. This helps you focus on only the data you need.

Customize Table and Graph Settings

When NSA generates Profile based Reports by default, the report output might either not show the entire data or show excessive data. Therefore, it is a good idea to customize the number of records in the Table and Graph settings to obtain the reports with the desired information.

Table Details: Enter the number of records that should appear in the profile based tabular report. You can opt to display any number of records from 10 to 5000.

Enter the number of sub-records records that should appear in the profile based tabular report. You can opt to display any number of sub-records from 1 to 500.

Graph Details: Enter the number of records that should appear in the profile based graphical report. You can display up to 24 records. Enter the number of sub-records records that should appear in the profile based graphical report. You can display up to 10 sub-records.

New Report

A custom report can be created by including only selected queries that meet your specific requirements. This helps you focus on only the required data. To create a new report, follow the steps below:

1. Enter the name by which you want the report known in the **Report Name** text box.
2. Select the queries you want to include in the report from the available report query list.
3. Click **Save** to save the custom report. This report is saved and is displayed in the Report List. To generate this report, just select it from the report list.

Editing a Report

To edit the settings for a report, follow the steps given below:

1. Select a report and click **Edit**. The **Edit Report** screen opens.
2. After making the changes, click **Save**.

NOTE: Any changes made will be reflected in the report, the next time it is generated. Default reports like Complete Report, Bandwidth Report, Protocol Report, Event Report, Intranet Report, and Device Report cannot be edited or deleted.

Deleting a Report

To delete a report, follow the steps given below:

1. Select a report from the report list and click **Delete**.
2. Click **OK** to confirm the deletion.

Save Report

Use this screen to specify the report name, the e-mail addresses to which the reports can be e-mailed automatically, and the remote FTP location to which your report can be uploaded. By default, the generated report is saved on the machine where NSA is installed in the following location.

[InstalledPath]\userprofiles\[user]\ProfileseIQ\[Profile name]\ [filename]

NOTE: It is recommended that you do not use mapped network drives to store generated reports. Instead use only your local drives to store the reports.

Reports are delivered in the following three ways:

- Saved on a local system or network neighborhood
- E-mailed to one or more recipients
- Uploaded via FTP to a remote location

The following sections explain how to specify the output and delivery of reports in each of these three ways.

Saving Reports

By default NSA saves a generated report in the machine where NSA is installed. For help on using generic file names, see the table below for examples.

Using Generic Names for Reports

NSA follows a generic method for specifying input and output file names in the profile. You can enter generic file names directly in name text box or you can use the Grammar Syntax feature to specify input and output file names. This feature is useful in scheduling repetitive tasks as the log file name is structured on a timestamp format.

File Specification Grammar Macro

Macro (Code)	Description	Format
%b%	Abbreviated month name	(Jan-Dec)
%B%	Full month name	(January-December)
%m%	Month	(01 – 12)
%d%	Day of month	(01 – 31)
%H%	Hour in 24-hour format	(00 – 23)
%y%	Year without century	(00..99)
%Y%	Year with century	(2000-2099)

NSA provides the option of using wild card specification in the file name, and understands standard DOS directory wild cards (i.e. , *). You can specify the relative hour, day, month or year by decreasing or increasing the specific value. The same syntax is used to specify file names for output reports.

Generic Naming – Grammar Syntax Examples		
File Name Specification	Sample File Name+	Represents
eIQ%m%%d%%y%.log	eIQ062009.log	June 20, 2009
eIQ%m%%d%%Y%.log	eIQ06202009.log	June 20, 2009
eIQ%Y%%d%%B%.log	eIQ200920June.log	June 20, 2009
eIQ%*%%m%%y%.log++	eIQ*0609.log	June 20, 2009

+ Assuming current date is June 20th, 2009

+ + In this example, all files created in June 2009 that are in the specified directory will be processed by the scheduler. This is because of the wild card specification * in the File Name. Note that NSA will not limit itself to files with only the day of the month. The wild card is a system wild card, and as in the DOS directory command, it will pick up all files with any matching string in place of the asterisk.

To specify file names using the Grammar syntax feature, follow the steps given below:

1. Click **New Profile** and select the second option to migrate log file data to the NSA database and generate a report. Click **Next**.
2. Click **Grammar**. The Grammar dialog box is displayed.
3. In the **Grammar** dialog box, click **Browse** and go to the location where generic log files are stored.
4. Define the timestamp format for the generically named files. Based on the log file naming convention of your log file, specify the appropriate date format in the Date Format text box. Note that you can add an alphabetical prefix to the format and select from several different file extensions in the suffix box.
5. In the Add/Subtract text box (Hour, Day, Month and Year) specify which timestamped log file is the input. For example, to attach to yesterday's log file, enter –1 in the Day text box with respect to the current system date.

E-mailing Reports

You can e-mail your reports to specified addresses using NSA. You can enter multiple e-mail addresses separated by semi-colons. Follow the steps given below to e-mail your reports:

1. Select the **Mail To** check box and enter the e-mail address in the text box. To e-mail to multiple recipients, use semi-colon to separate the e-mail addresses.
2. You can enter multiple e-mail addresses separated by semi-colons and send a copy of the report to other users (cc :) if required.

3. Enter the subject in the **Subject** box.

TIP: This feature will work only if your SMTP server is configured.

FTP Reports

You can also choose to upload your report to a remote FTP location. Follow the steps given below to upload your reports:

1. Select the **FTP** check box and enter the host name to send the file, user name, and password to configure FTP. The machine that is to receive the reports must be running an FTP service.
2. Select the **Passive Mode** check box if you want NSA to use "passive FTP" to initiate FTP connections.
3. Passive FTP connections provide more security for the network that hosts the FTP server to which NSA will connect. Clients that use passive FTP send a PASV command, which allows the server to specify which data port it wants to use, rather than sending a standard POST command to specify a control channel and data channel port.

Edit Profile

You can edit or delete a profile as required. To edit a profile, follow the steps described below:

1. From the menu bar, click **Edit Profile**.
2. On the **Edit Profile** wizard you can edit the configuration settings made in **Device**, **DNS Lookup**, **Filter Templates** and **Reports** tab respectively.
3. Click **Save to** save the settings.

Copy Profile

If you want to create profiles that are similar, use the copy profile option.

1. To create a copy of a profile, select an existing profile and click the **Copy Profile** button on the main screen.
2. The Copy Profile window opens displaying the newly created profile.

The profile created is identical with the former except the profile name.

Delete Profile

To delete a profile:

1 Select the required profile you want to delete and click **Delete**.

2 You are prompted for confirmation. Click **Yes** to confirm the deletion.

Chapter 16: Forensics

Forensics analysis involves recording and analyzing network events in order to discover the source of security attacks or other problem incidents.

It involves capturing of all data packets passing through a certain traffic point and written onto a storage area (file archive) with analysis being done subsequently in batch mode. This approach requires large amounts of memory storage (SAN or NAS), involving a file system.

NSA's forensics analysis uses this approach to perform the forensics analysis and in this the major concern is for privacy as all packet information including user data is captured. NSA addresses this by using a secure communication channel when collecting the logs from the specified devices and saving them for forensic purposes.

The Forensics analysis feature helps you to look up a metadata index for specific information across devices across up to several years. This metadata index contains information such as the device ID and time range that references each log file. This enables NSA to quickly refer log files that contain the device ID and time range applicable to the search.

A configured search has the following columns associated with it.

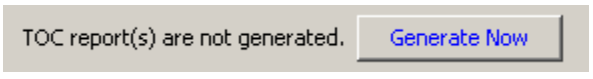
- Search Name
- Report Generated
- Archive
- Generate Report

You can edit, copy, or delete a defined searching criterion.

Report Generated: Click the link under the Report Generated column to view the report. You can also customize the report view by including only those fields you want to view.

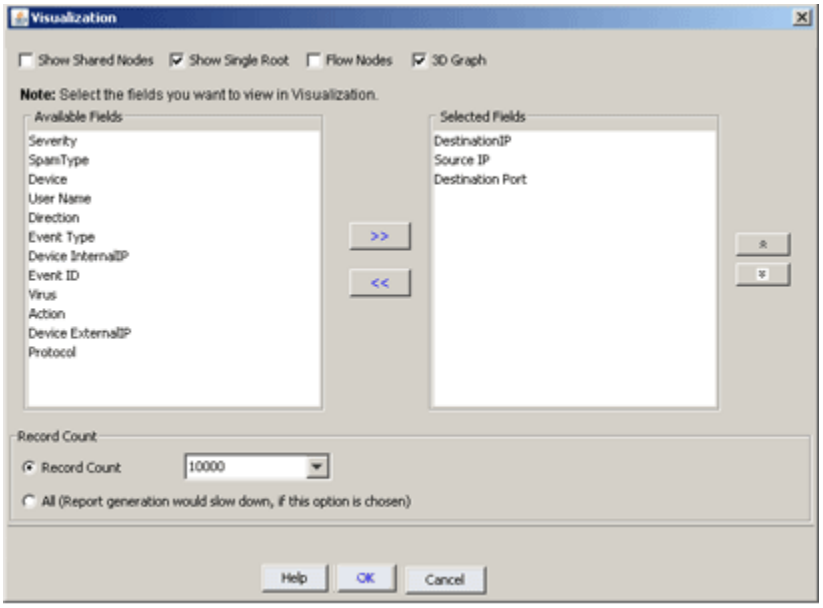
Use the following options to customize your report view:

- **Generate Forensic TOC** - When you generate a forensic report on the configured search for the first time, reports shown in the TOC are not generated. Click on the **Generate Now** button to generate the TOC reports.



- **Number of Records** - To change the number of records you want to display in the report.
- **From-To** - To specify records within a range.
  Note: The specified range cannot exceed more than 1000 records.
- **Export Report** - To save your search result in either HTML/Text formats.

Note: Values in a report saved in text format are separated by a comma separator.



NOTE: Forensics analysis stops if the available disk space is less than 20% of the total disk space. Once the disk space falls below this level, the following message appears: *Stopped Forensics searching due to unavailability of free disk space.*

Export Report:

You can export the forensic report to be saved onto a specific location and in HTML or Text format. To customize the view of the exported report, select the fields you want to include in the report that is being exported.

NOTE: Values in a report saved in text format are separated by a comma separator.

Follow the steps described below to export a report:

1. Click **Export Report**. The Export Report screen opens.
2. Select the **Report Type** you want it to be exported to.
3. Select the fields you want to view from the **Available Fields** list and click to move them into the **Selected Fields** list.
4. Select the range of records that you want to export from the generated forensic report.
5. Click **Export**.

NOTE: In Forensics reporting, number of records displayed in graphs is limited to 11.

Archive: This column displays the details of the latest results of the configured search. Once a new update for this search is triggered, search results for this search are transferred to the archives.

Generate Report: This column displays the report icon. Click  to generate a report for the configured search.

Log Collection

Using forensics analysis, you can specify from what devices to search log files. In addition, you can do the following:

1. Collect log files from all configured devices.
2. Store logs in OLF (Open Log Format) and compress them into delta files.
3. Transfer delta files from the Data Collector to the Forensics Analyzer database.
4. Select the format and the location where you want the logs saved from the Options screen.
5. Select a time period to search for specific information.

Configuring Search

The following sections explain how to configure a new forensics search.

New Search

1. On the Forensics Manager window, click **New**. The New Search wizard opens. To edit a forensics search, select a configured search and click **Edit**.
2. Enter a name and description for the search in the Name and Search box respectively. While editing, you can only change the description.
3. Select the criteria of your search. You can select a search criterion for Forensic log analysis.
4. Select the criteria (source)—Device on which you want to perform the forensic search.
5. Select from one of the following log sources you want to search from:
    - Log Files from Selected Devices
    - Archived Search Data
    - Raw Forensics (Only for BlueCoat device(s))
    - Cisco Mars
6. Click **Next**.

Archived Search Data

If you have selected this option as the log source for your search, your search is confined to the data present in the reports previously generated. This helps you save time as you need not search the entire log database.

1. Browse to the location where previous reports are archived to search for the required data and click **Next**.

NOTE: If no report is generated prior to this search, archived data is not available for you to lookup. So this option will not be functional.

Browse Server

1. Click **Browse** and the **Browse Server** Window opens.
2. This window gives you the directory hierarchy of the machine where the NSA Server is installed.
3. You can select a folder by double-clicking any item or by Selecting the folders under  icon and click **Open Folder** to view the files within the folder in the under Files section.
4. Similarly, you can select and add a file within a selected folder by double-clicking it or by clicking the **Add File** button.
5. Selected log files will be listed under Selected Log Files section.
6. To remove a selected file, click **Remove File** button.
7. You can see the path of your selected file or folder in the Selected Log Files section and click **OK**.

Raw Forensics

To perform a forensic search on the BlueCoat device, use the Raw Forensics option as the source of input. The raw logs from the BlueCoat device are fetched every half an hour and stored in the Forensic folder of the application. NSA supports Raw Forensics on BlueCoat logs that are in the following file format with specific header information:

```
#Software: SGOS 3.2.4.8
#Version: 1.0
#Date: 2005-09-28 02:31:13
#Fields: date time time-taken c-ip sc-status s-action sc-bytes cs-bytes cs-method cs-uri-scheme cs-host cs-uri-path cs-uri-query cs-username s-hierarchy s-supplier-name rs(Content-Type) cs(User-Agent) sc-filter-result sc-filter-category x-virus-id s-ip s-sitename
```

Log Files from Selected Devices

If you have selected this option as the log source for your search, Click Next and follow the steps described below:

New Search (Device)

Date & Time Range

You can enter the time period to configure your search. Follow the steps described below:

1. Select any one of the options given below to restrict the search to specific day(s):
    - Today,
    - Yesterday
    - All Dates
    - Specify Date
2. If you select Specify Date, the **From** and **To** fields are activated. Enter the starting and ending date by using the calendar icon
3. Select the time of the day from the drop-down list available.
4. Click **Next**.

Scheduling Forensics Search

The Scheduler facilitates you to run the forensics search reports automatically, at specific times, which is particularly advantageous when you are running reports at regular intervals.

In the new profile wizard, select the **Scheduler** tab and the scheduler screen opens. The list box contains all the tasks that are scheduled. Click the **Add** button to schedule a new task or select an existing task to edit.

Add Task

1. Click the **Add** button. The **Scheduler Frequency Selection** screen opens.
2. On this screen, you can select the frequency at which you want the forensics report to run.
3. Specify a unique name for the task in the **Task Name** box. This name is displayed in the Scheduler Main Window under the column Scheduled Tasks.
4. Select the frequency from the options given. The available frequencies are:
    - Daily
    - Weekly
    - One Time Only
5. The forensics report schedule you just created is added to the list of scheduled tasks in the Scheduler screen of configure forensics search wizard.

NOTE: Hourly and Monthly tasks configured in the earlier versions are no longer supported after the upgrade and need to be edited to acquire a different frequency to run the scheduled task.

Choose Nodes

You can select respective nodes and analyze their logs. Whatever is the criterion selected in the opening screen of new forensic search screen, the corresponding window opens. For

example, if your chosen criterion is Device, the corresponding window displays all the devices licensed with NSA.

1. To select individual network Devices, select the check box against the device name.
2. Click **Next**.

Set Criteria - Filters

You can select the filters you want to apply on your search from here.

The following are the available filters:

- Destination
- Destination Port
- Event ID
- Event Description
- Protocol
- Rule
- Severity
- Source
- URL
- Virus Name
- Flow
- Content Category
- Action
- Attack Type
- User Name
- Status Code
- Facility

Source Filter

If you have selected Source filter, follow the steps described below:

1. Enter the Source IP/Name of the device you want to filter from the rest and report on only those events originating from the specified source.
2. To filter on events originating simultaneously from a series of devices, specify the IP Range by selecting the Source IP Range check box.
3. Add the Source IP/Name by clicking the **Add** button.
4. Click **Save Filter**.

Destination Filter

If you have selected Destination in the Search Filters window, follow the steps described below:

1. Enter the Destination IP/Name of the device you want to filter from the rest and report on only those events having the specified Destination IP/Name.
2. If you have to filter on events from a series of devices at one time then you can provide the IP Range by selecting the Destination IP Range check box.
3. Add the Destination IP/Name of the device or the range by clicking the **Add** button.
4. Click **Save Filter**.

Destination Port Filter

If you have selected Destination Port in the Search Filters window, follow the steps described below:

1. Enter the Destination Port number in a device that you want to filter and report on only those events ending up in the specified port.
2. Add the port number by clicking the **Add** button.
3. Click **Save Filter**.

Rule Filter

If you have selected Rule in the Search Filters window, follow the steps described below:

1. Enter the Rule ID you want to filter and click **Add** to move them into the Selected Rules list.
2. Click **Save Filter**.

Protocol Filter

If you have selected Protocol in the Search Filters window, follow the steps described below:

1. Select the protocols you want to filter and click  to move them into the Selected Protocols list. You can also add new protocols.
2. Click **Save Filter**.

Event ID

If you have selected Event ID in the Search Filters window, follow the steps described below:

1. Select the Event IDs you want to filter from the available list below.
2. Click **Add** button to add a new event ID to the list.
3. Click **Add** to open the New Event ID screen.
4. Enter an appropriate name and the ID of a new event you want to add to the list.
5. Click the **Add** button and click **Save Filter**. The new event ID is added to the list of existing event IDs.
6. Click **Next**.

Event Description

If you have selected Event Description in the Search Filters window, follow the steps described below:

1. Enter the event description as a Regular Expression to search for in the database.
2. Click **Save Filter** button.

Severity Filter

1. You can select the severity types which you want to filter in your search from this screen.
2. Available severity types are:
    - Emergency
    - Alert
    - Critical
    - Error
    - Warning
    - Notice
    - Information
    - Debug
3. Select from the Available severity types and click  to move them into the Selected Severity Types list.
4. Click **Next**.

URL

You can search for any item containing a specific URL, word or phrase from the database.

1. Enter the URL as a Regular Expression to search for the specified addresses in the database.
2. Click **Add** and then click **Save Filter** button.

Virus Name

You can search for any item containing a specific Virus Name from the database.

1. Enter the Regular Expression of the Virus Name, word or phrase to search for in the database.
2. Click **Add** and then click **Save Filter** button.

Flow

If you have selected Flow, follow the steps described below:

1. Select from the following
    - Inbound
    - Outbound
2. Select Inbound if you want to filter only incoming events.
3. Select Outbound if you want filter only outgoing events.

Content Category

You can search for any item containing a specific Word or Phrase from the database for the content category.

1. Enter the Regular Expression of the content category type to search for in the database.
2. Click **Add** and then click **Save Filter** button.

Action

The Action details include the Allowed or Denied events.

1. Select an Action from the action details to filter.
    - Allowed
    - Denied
2. Click the **Save Filter** button. The filter is added to the Filter list.
3. Click the **Delete** button to clear the settings.

Attack Type

If you have selected Attack Types, follow the steps described below:

1. Select the Event Types you want to associate with the monitor from the Available Attack Types list.
2. Click  to transfer the event types to the Selected Attack Types list.
3. Click **Next**.

User Name

You can search for any item containing a specific User Name from the database.

1. Enter the Regular Expression of the Virus Name, word or phrase to search for in the database.
2. Click **Add** and then click **Save Filter** button.

Status Code

You can search for any item containing a specific status code from the database.

1. Enter the Status Code to search in the database.
2. Click **Add** and then click **Save Filter** button.

Facility

This screen allows you to select the Facilities which you want to filter in your search.

1. Available Facilities are System, Security, Application, DNS Server, Directory Service, File Replication, Kern, User, Mail, Daemon, Auth, syslog, Lpr, News, UUCP, Cron, Authpriv, Ftp, Local0 through Local7and Mark.
2. Select from the available Facilities and click to move them into the Selected Entities list.
3. Click on **Save Filter** button.

Report Output

When the search is finished, follow the steps described below to choose the fields you want to include in the report:

1. Select the fields you want to include from the Available Fields and click  to move them into the Selected Fields list.
2. To include a column in the forensics report for including the native log, select the check box **Append a column in the forensics report for including the native log**.
3. Click **Next**.

Create Expression

Once you define the Criteria (s), you can combine/negate/select the criteria within the Search by using the following operators:

1. The list of criteria defined for the search is displayed in the Identified Criteria list.
2. You can use the "And" operator to select and combine more than one criteria to apply in unison to the Rule.
    - Select criteria from the list. For example —Select CRITERIA 1.
    - Select the complementary criteria from the list. For example—select CRITERIA 2.
    - Click the And operator.
    - Click Finish.
    - The Operator settings appear in the Summary text box.
    - In this case — (CRITERIA 1&&CRITERIA 2). Now both the criteria are combined and will be executed in unison.
    - The "And" operator is denoted by an ampersand symbol (&&)
    - Click Clear Expression to undo the Operator settings.
3. You can use the "Or" operator to select two or more than two criteria and apply one of them to the Rule.
    - Select a criteria from the existing list. For example - Select CRITERIA 1.
    - Select the complementary criteria from the list. For example—select CRITERIA 2.
    - Click the "Or" operator.
    - Click Finish.
    - The Operator settings appear in the Summary text box.
    - In this case - (CRITERIA1||CRITERIA2). Now both the rules are combined and the one which meets the criteria first will be executed and the other stands void.
    - The "Or" operator is denoted by a pipe (vertical bar) symbol (||)
    - Click **Clear** to undo the Operator settings.
4. Press the Ctrl key and select more than one criteria at a time from the existing criteria list and click the operator you want to apply from the available operators except the negate filter. As the Negate operator works on one filter at a time.
5. By default the "Or" Operator is applied to the filter.

6. **Negate**: Use this operator to negate the Regular Expression that is built by applying "Or" and "And" operators on the selected criteria. The negated Regular Expression appears prefixed with an exclamation symbol -"!".
7. Click **Next**.

Save Report

Forensics Reports for devices can be saved in the following two ways:

- E-mailed to one or more recipients
- Uploaded via FTP to a remote location

The report can be saved to the specified location either in Text or HTML formats. Follow the steps given below to e-mail your forensic reports:

- Select the Mail To check box and enter the e-mail address in the text box. To e-mail to multiple recipients, use comma to separate the e-mail addresses.
- You can enter multiple e-mail addresses separated by comma and send a copy of the report to other users (cc:) if required.
- Enter the subject of the mail.

Follow the steps given below to FTP your forensic reports:

1. Select the FTP check box and enter the Host name to send the file, User Name, and password to configure FTP. The host machine should have FTP service running in it.
2. Select the Passive Mode check box if you want NSA to use "passive FTP" to initiate FTP connections.

NOTE:
- Take caution in using Mail To and/or FTP options for saving the forensic report as the report can be voluminous.
- MHTML report generation depends on the available system resources. So there is a possibility of report generation to fail if the report contains more than half-million records.

Set Permissions

Admin Users: By default all NSA admin users will have access to all search profiles. Any logged in admin user can Edit the settings of the policy, Save the settings of the search. It is up to this Admin User discretion whether to allow SRM power users to View this Policy and able to Edit or Delete this policy.

Power Users: The Power users have only Read-Only Permissions. Hence these policies are loaded to this user but cannot edit or modify anything.

User Defined Polices: If the power user creates a New Search, then this user will automatically become the owner of the policy, this user can define access settings for other power users using the permit other users using the Set User Permissions option present in the Create Policy window.

By default the User creating the policy will have All privileges on the Policy i.e., View, Edit and Delete.

Summarizing the Permissions Scenario

User with:

- Read -> can view the search settings as well as alert-archives
- Edit -> can change the filters (Read + Acknowledge + Clear)
- Delete -> can delete the search (Read + Acknowledge + Clear + Edit + Delete)

To make any changes before saving it, click the **Previous** button.
To complete the process, click **Finish**.

Edit Search

Follow the steps described below to edit a configured search:

1. Click a search under the column **Search Name**. The **Edit Search** window displays.
2. Make the necessary changes and click **Next**.
3. Verify the altered settings and click **Finish**.

Copy Search

To create a copy of an already existing search, use the Copy Search option. Follow the steps described below to create a copy:

1. To create a copy of a search, select an existing search and click the **Copy Search** button on the main screen.
2. The **Copy Search** window opens displaying the newly created search.

NOTE: The search just created is identical to the former except the search name.

Delete Search

To delete a search,

1. Select an existing search and click the **Delete** button on the main window of Forensics manager.
2. You are prompted for confirmation. Click **Yes** to confirm the deletion.

Forensics Options

With the Forensics options you can specify the path where you want to store the forensics logs. You can choose to be alerted whenever your secondary storage device falls below the specified level.

Follow the steps described below to set your options for forensics analysis:

1. On the main window, click **Options**. **The Forensic Options** dialog box opens.
2. Specify the Path where you want to store the forensic logs by clicking on Browse button.
3. Select the folder where log files are stored and click **OK**.
4. You can also specify the data retention period for the forensic logs using the Data Retention Period in months. By default the field has value '-1' which indicates permanent storage of data.

Note: The change in the retention period will be effective in the next 12 hours or the next NSA Service restart, whichever is earlier.

Disk Space Alert: Forensics analysis may stop due to unavailability of free disk space. To restart it, you can free up the disk space or specify a different location from the Forensics > Options tab.

1. Select the **Disk Space Alert** check box to raise an e-mail alert if the memory percentage available is less than a pre-defined value.
2. Enter the recipient e-mail address in the **Mail To** box. To add a copy, enter an e-mail address in the Cc box. Use comma to separate multiple e-mail addresses.
3. Click **Save**.

NOTE: - Forensics analysis will stop if the available disk space is less than 20%.
- To be able to send an e-mail alert, your SMTP server must be configured.

TIP: To see the mapped network drives created by the user, change the service logon properties from Local System account to This account with a valid username and password from the Service Control Manager.

Chapter 17: Dashboard

Dashboard Manager delivers monitoring and reporting metrics—so authorized security personnel in the organization can monitor and understand the security posture of your network. Easy to build and user friendly, NSA dashboards give a quick birds view of your existing network infrastructure for deep analysis of security measures. By managing dashboards, you can track metrics, gain insight from underlying analysis, and can alter rules as conditions change. Dashboard Manager provides you with a consistent and accurate way to monitor critical security areas.

The default Dashboard screen comprises of various distinct panels that gives you an overview of following activity in your network:

- Event Viewer
- Top Sources
- Direction Chart
- Total Events
- Top Destinations
- Port Activity
- Top Attacks By Events By Victim
- Event Action Chart

Design Options in Default Dashboard panels

There are two kinds of panels on the dashboard— Monitors and Reports. Each panel has the following options for reworking on the look and feel of the monitor. Click the icon in the dashboard panel, the following expandable list of options appear:

 **Snap**: Use this option to capture a screen shot of the dashboard pane. NSA saves a copy of the snaps every one hour in a day, in chronological order. You can compare snaps taken at different times to evaluate the periodic status of the desired events on your Devices. Hold the ctrl key and select the time stamps of the snaps, the right pane displays the selected snaps adjacently, making it easy for you to track down the differences between them. You can simultaneously compare up to 12 snaps at one time.

 **Zoom**: Use this option to maximize the current view.

 **Modify**: Use this option to modify the information displayed on the pane. Click on the icon, the Modify Dashboard View window opens, which displays the list of other view options. Select the information option from the list that you want to view in the Dashboard and click **OK**.

This option is useful when you have to replace any of the dashboard panels with a new one without altering the placement of existing panels.

Drilldown: Use this option to delve into the information of the selected monitor. This is extremely useful when you want to generate a quick report and find out what contributed to the numbers present in the reports.

Table: Use this option to present the information of the selected monitor in a tabular format.

NOTE: If the number of Graph attributes for a monitor is more than twelve, its corresponding information cannot be shown in tabular format.

Graph: Use this option to present the information in different visual forms. You can opt to see the information in table and different graph types— Bar, Tape, Pie, Horizontal, Line, Radar and more. If you select more from the collapsible list of graph, the More Graph Types window opens, where you can select from visually delightful various graph options like—Bar, 3DBar, Gauge, Horizontal, 2DLine, 3DLine, PIE, Radar, 2DArea, 3DArea.

View By: Use the View By option to generate monitor classified by Hits or Bytes.

Show Legend: Use this option to see Graph Legends, which are a key to the data plotted on the graph; on the dashboard panel.

Show Table: Use this option to see the information in a tabular form. The Show Table option is available on the graph monitors only. On selection of this option the table is shown below the graph.

Customizing Dashboard View

With the choice to create personalized views, Dashboards are no longer exclusive to security administrators. As all role-based users need access to relevant security information in order to make right decisions, with Dashboard Manager, users can build personalized dashboards that give the information they need. Various personalization options make it easy to create custom dashboards for different users or groups of users.

The various options available under **Add/Edit a Dashboard** drop-down list are as follows:

To create new dashboard- Use this tool to create customized dashboards to view the reports on desired information on performance counter of devices in a single view.

To set current view as default view- If you have created a customized dashboard displaying information you need most and would want to monitor it regularly, then you can set that dashboard as the default view. Henceforth, the performance monitoring portal will open with the default view.

To restore factory defined default view- Use this tool to restore the factory defined default view from the customized dashboard.

To delete dashboard: Network activity is dynamic in nature; therefore, what was required yesterday might become obsolete today. To keep pace with the changing information you can delete the unwanted dashboards by clicking on this icon.

To copy dashboard- If you want to instantly make a copy of the current dashboard, click on this icon, a dashboard pop-up comes up, prompting you to save the copy of the dashboard. By default, the name of the copy of the dashboard is saved in Copy_of_<dashboard name> syntax. You can enter the name of your choice in the dialogue box and Click OK to save the copy of the dashboard.

To change to design/run mode for resizing monitors- NSA gives you extreme flexibility to change the look and feel of the customized dashboard. Open any customized dashboard that you have created and click this toggle button to activate the design mode, and you can resize, drag and drop the individual monitors to arrive at a dashboard of your choice. The selection of this icon adds a few more tools that aid in designing a customized dashboard:

Tools to Edit Dashboard in Design Mode

To add panel to current dashboard: If you want to instantly add a panel to the current dashboard, click on this icon, the add dashboard panel window opens. Select the desired queries for which who want to add a panel (s) to the current dashboard. You can opt to add device based panels of your choice to the dashboard.

To save dashboard: Once you have redesigned your customized dashboard with chosen panels in desired size and position, you can save those settings by clicking on this icon.

Layout Design Tools: NSA provides easy-to-use, one click tools to resize and re-align the selected panels to create a desired layout on the dashboard. The following tool list appears, when the dashboard is in the design mode:

Hold the ctrl key and select the panels that you want to resize or re-align. Select the panel that you want to set as a precedent in the end. And click the desired tool from the collapsible list, for example if you want to resize the width, collapsible list and all the selected panels width will be resized to the panel selected in the end. You can adjust multiple panels at a time by selecting them in succession by holding the ctrl Key.

NOTE: If your current selection is the default dashboard, then icon appears in a disabled state. You cannot resize or re-align the panels on the default dashboard, instead you can use task bar to modify the information displayed on the individual panels.

Add Dashboard Panel

NSA provides you the flexibility to add a panel to the current dashboard instantly. Follow the steps given below to add a new dashboard panel to the current customized dashboard:

1. Click on **Add panel** option icon from the dashboard design menu, the add dashboard panel window opens.
2. Select the desired report or monitor for which you want to add a panel (s) to the current dashboard.
3. You can add device based panels of your choice to the dashboard.

On the Default Dashboard you can view the general summary of the nodes being monitored by NSA.

Create Dashboard

A dashboard is a user interface that organizes and presents complex information in a way that is easy to comprehend. NSA comes with an interactive, user friendly Dashboard comprising of viewing panes -- Real-Time Events, Event Graphs, Alert Graphs etc.

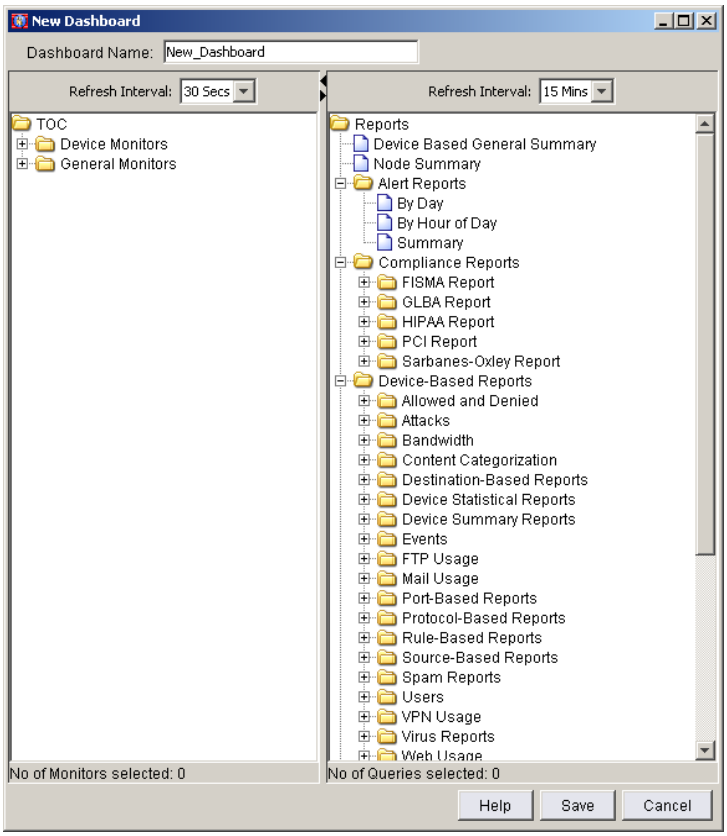
How to Manage?

On the dashboard main screen, the Dashboards drop-down lists containing all the dashboard views is available to the user.

To set a view as the default, select from the drop-down list and click the set as default option. To restore the default dashboard view, click the **Restore Dashboard** option.

Creating New Dashboard

You can create customized dashboards to view the reports and monitors on desired information of devices at once.



Follow the steps given below to create a customized Dashboard:

1. On the dashboard options menu, select the new dashboard option. The create New Dashboard wizard opens.
2. Enter a Dashboard Name for your customized dashboard.
3. Select the Monitors and Reports that you want to be part of the dashboard.
4. Select the monitors you want to set in the dashboard view from the Monitoring TOC.
5. Select the query (s) to generate a report on the selected monitor from the Reports pane. Hold the ctrl key and select the reports to view in the dashboard, click **Save**. The created Dashboard is populated in the Dashboard drop-down list.
6. Click **Save**. The dashboard view is saved and listed in the dashboards drop-down list.

NOTE: By default, dashboard view is opened in the Run Mode. To change the mode to Design Mode, click the design mode option, resize or rearrange the monitors available on your dashboard view and then click on the mode icon to restore the run mode.

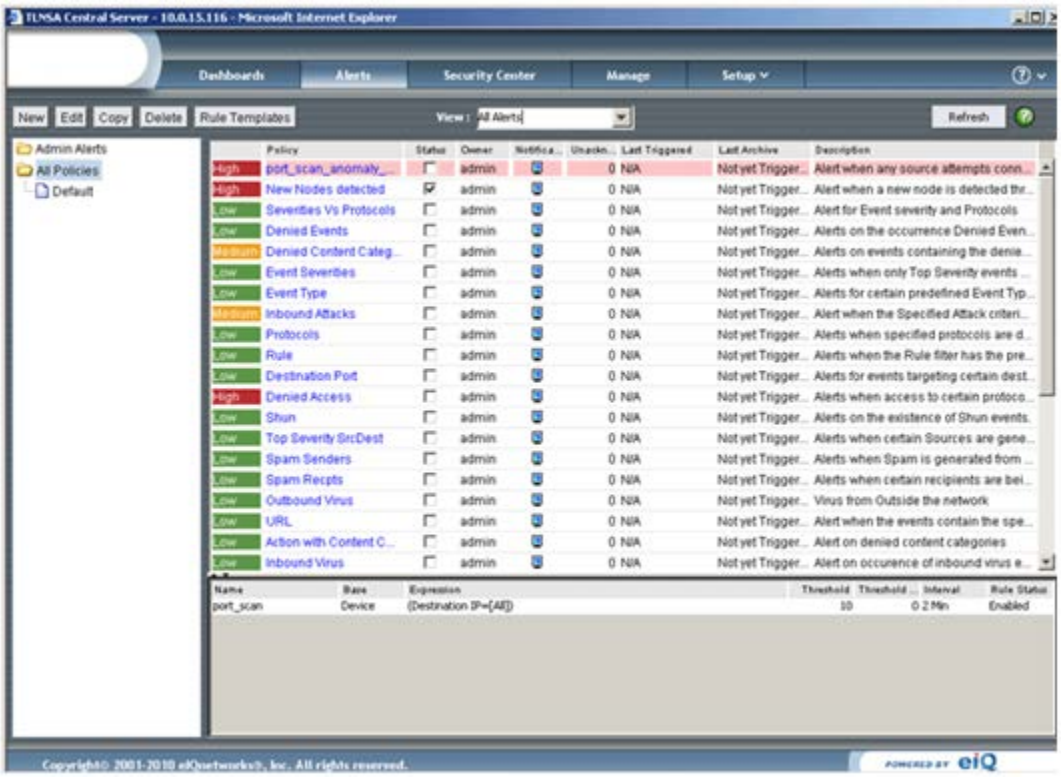
Chapter 18: Alerts

Security analysis and administration depend on implementation of modules. Each module in NSA may be governed by one or more users. By the usage of workflow, you can automate the interactions among NSA users by providing a common platform where they can raise issues in the implementation by lodging and assigning tickets. Concerned NSA user will take necessary actions based on the lodged ticket to rectify the anomaly in the implementation, update the same as comment and thereby fixing the issue.

Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, where the information is monitored; others are active, where the information is altered with intent to corrupt or destroy the data or the network itself. The Alerts feature of NSA provides warning in advance so you can respond proactively.

The **Alerts** module displays the list of all the Alerts configured to the Policies. The Alert Name corresponds to the name of the Policy for which it is enabled. The alerts warn you whenever a specified event type or attack activity is detected or if the total number of attack attempts exceeds a specified value.

The Alert Manager



IMPORTANT: A Console user, given the Access Using Console privilege to monitor alerts of a specific user will only see triggered alerts for that user.

Add To Group

All the factory defined policies are placed under the Default Group. If the user wants to categorize the existing Alert Polices or User Defined Alert Polices under a new group, use the **Add To Group** option.

Follow the steps given below to add an alert policy to group:

1. Right-click on the alert policy that is to be added under a group.
2. All the existing groups in the Groups tab are displayed in the menu bar other than the default group.
3. Select the Add to -> New Group option if you want to create a new group or select an existing group to which you want to include the Alert Policy.

The main menu bar of the Alerts window contains the buttons to add a New Alert based Policy, Edit, Copy and Delete Alert based Policies. It also includes a button to create Rule Templates.

View: By default NSA installs with in-built alert policies. The number of default and customized policies put together can become difficult to track and manage. Therefore, the View drop-down list can help you display the policies classified based on the criteria on which they were defined. This helps you in filtering policies, which are Enabled/Disabled and Triggered alerts.

- All
- Enabled
- Disabled
- Triggered

For example, if you select Alerts from the View list, the page will display only the Alert based policies.

Search:

You can perform a quick search to locate any particular alert by entering a search string. For Example: If you want to locate an alert, enter its name in the Search text box and press the Ctrl key. The relevant Alert will be highlighted.

An Alert Manager displays the following information pertaining to an Alert. Also you can double-click on an Alert from the Alert manager to open up the Alerts Workbench for the alert.

- **Alert Name**: The Alert name corresponds to the Policy name. For example, if an Alert is configured on a policy called Policy1, the Alert name will also be Policy1. You can sort this column based on alphabetical order.
- **Alert Description**: Alert description displays the description of the corresponding Policy.
- **Alert Notification**: This displays the method of Alert notification opted by you in the Policies. You can either notify Alerts via e-mail or by SNMP trap; if none is specified then "on screen" notification is displayed.
- **Unacknowledged Events**: This displays the count of events which are filtered through Rules to be a part of the Policy. As NSA encounters these events they are marked as unacknowledged events and are displayed here. You can clear each event by clicking on that field (number). With every event you acknowledge and clear the count decreases by one alternatively you can acknowledge and clear all events at once. Click on the unacknowledged events column label to sort the unacknowledged events count in a descending order.
- **Last Triggered Time**: This column displays the date and time when the Alert was last triggered.
- **Last Archive**: This column informs about the status of the Alert. If the Alert criterion is not met then "Not yet triggered" message is displayed. The triggered Alert is archived and the message shown in that case is "Archive". You can click on "Archive" to see the corresponding details of the archived Alert. Go to **Alert Archive** for more details. You can also sort this column based on Archive or Not Yet Triggered criteria.

Create Alert Policy

Basic Information

From the Alerts module, you can define new policies for triggering alerts and Notify users

1. Click **New** from the **Alerts** module on the main window, the New Policy wizard opens.
2. Enter a Policy Name.
3. Select a group under which the alert policy should be placed from the **Policy Group** drop-down. By default, a new policy will be placed in the **Default Group**. To create custom group, click here for details.
4. Enter a short description of the Policy properties for future reference and the Impact of the Policy on the network once it is implemented and the proposed Remedy if it is a threat to the network security.
5. Associate a Severity level to the Policy. The severity level is reflected in the Alerts window, once you create and save the Alert Policy. The options available are as follows:
    - Low
    - Medium
    - High.
6. Click **Next**.

Schedule Policy

In the new policy wizard from the schedule policy screen, you can specify the time during which the policy will be enabled.

1. If you want the policy to be enabled at all times, select the option “This policy will be enabled 24 hours a day”.
2. If you want the policy to be enabled only between the specified times, select the option This policy will be enabled during these times (use 24-hour time).
3. Enter a Time Range by selecting the time from **From** and **To** drop-down time list and specify the time span within which you want to enable the Policy. Click **Add this time to schedule** button and the time range is populated in the Schedule box. You can add multiple Time Ranges to enable the Policy more than once in a day.
4. If you want to remove a time range, select the entry from the schedule box and click **Delete this time** button.

Set Rules

In the new policy wizard from the Set Rules screen, you can specify to create New Rule, Edit Rule, Copy Rule, Delete Rule and Advanced Rule Options. This window displays the list of Rules available for the Policy. Based on the requirement, each rule of the policy can either be enabled or disabled.

New Rule - Basic Information

1. From the **Set Rules** screen, click **New Rule** button.
2. The New Rules Wizard opens. From here you can assign rules to a policy from two different sources, they are as follows:

   Import from template

   - Select the **Import From Templates** option from the Basic Information screen of the New Rule wizard.
   - Select the Rule Template to import from the available custom made Rule Templates list. To import more than one templates press the Ctrl key and select the Rule templates.
   - Create New Rule
   - Select the Create New Rule option from the Basic Information screen of the New Rule wizard.
   - Select the Rule Template to import from the available custom made Rule Templates list. To import more than one templates press the Ctrl key and select the Rule templates.
3. If a template is selected, the Rule Name and Rule Description fields will acquire the details as available in the template.
4. If **Create New Rule** option is selected, enter an appropriate Rule Name and a short but apt description about the rule in the **Rule Description** box.
5. Click **Next**.

Identify Criteria for the Rule

A rule is made up of one or more criteria that, when satisfied, trigger the rule. To create one, choose a category, then choose your criteria from the list and then click **Use this Criteria**. A rule should only contain criteria from one category.

Identifying Rule Criteria

- Device

Editing a Rule

1. Select the Rule that you want to edit from the Rule list populated on the Create Policy window. The column Base identifies whether the Rule is based on what criteria.
2. Click on the Edit Rule button from the Create Policy menu bar.
3. If you have selected a Device based rule to edit, the corresponding window opens. And if Similarly other edit rule window opens for the rule criteria you chose to edit.
4. The Rule name is non-editable.
5. You can edit the description of the Rule.
6. Make the necessary changes-- you can edit the settings on all the filters available in the list and also add new filters.
7. Click the **Next** button to proceed with editing process, else click the **Cancel** button to abort the task.
8. On the next screen if needed, you can change the way the operators are working on the sets of filters.
9. Click **Save** to save the edited Rule on the Create Policy window
10. Click **Save As Template** to save the edited rule as a template in the Rule Templates repository accessible from the Policies main window.
11. Click **Previous** to revert to the earlier screen to alter or recheck the filter settings.
12. Click **Cancel** to abort the task.

Making a Copy of the Rule

1. Select the Host Rule to make a copy of, from the Rule list populated on the Create Policy window. The column Base identifies whether the Rule is based on what criteria.
2. Click on the Copy Rule button from the Create Policy menu bar.
3. A copy of the selected rule is created.
4. The copy of the Rule is saved with a prefix "Copy_of_" followed by its original name.
5. You can edit the name and the description of the copy of the Rule.
6. You can edit any or all the filter settings followed by the operator settings pertaining to the original Rule and can also add new filters.
7. Click **Save** to save the Copy of the Rule on the Create Policy window.

8. Click **Save As Template** to save the Copy of the Rule as a template in the Rule Templates repository accessible from the Policies main window.
9. Click **Previous** to revert back to the earlier screen to alter or recheck the Device filters settings.
10. Click **Cancel** to abort the task.

Deleting a Rule

1. Select the Rule to delete from the Rule list populated on the Create Policy window.
2. Click the **Delete Rule** button from the Create Policy menu bar.
3. The dialog box prompts you for a confirmation. Click **Yes** to delete, **Cancel** to abort the task.
4. The Rule will be permanently deleted from the Policy.

Rule Expression

Once you create the Rule (s), you can combine/negate/select the criteria within the Rules by using the following operators:

1. The list of criteria defined for the rule is displayed in the Identified Criteria list.
2. You can use the "And" operator to select and combine more than one criteria to apply in unison to the Rule.
    - Select criteria from the list. For example —Select CRITERIA 1.
    - Select the complementary criteria from the list. For example—select CRITERIA 2.
    - Click the **And** operator.
    - Click **Finish**.
    - The Operator settings appear in the Summary text box.
    - In this case — (CRITERIA 1&&CRITERIA 2). Now both the criteria are combined and will be executed in unison.
    - The "And" operator is denoted by an ampersand symbol (&&)
    - Click Clear Expression to undo the Operator settings.
3. You can use the "Or" operator to select two or more than two criteria and apply one of them to the Rule.
    - Select criteria from the existing list. For example - Select CRITERIA 1.
    - Select the complementary criteria from the list. For example—select CRITERIA 2.
    - Click the "Or" operator.
    - Click **Finish**.
    - The Operator settings appear in the Summary text box.
    - In this case - (CRITERIA1||CRITERIA2). Now both the rules are combined and the one which meets the criteria first will be executed and the other stands void.
    - The "Or" operator is denoted by a pipe (vertical bar) symbol (||)
    - Click Clear to undo the Operator settings.
    - Press the Ctrl key and select more than one criteria at a time from the existing criteria list and click the operator you want to apply from the

available operators except the negate filter. As the Negate operator works on one filter at a time.
- By default the "Or" Operator is applied to the filter.

4. Negate: Use this operator to negate the Regular Expression that is built by applying "Or" and "And" operators on the selected criteria. The negated Regular Expression appears prefixed with an exclamation symbol -"!".

Choose Targets

1. The window displays licensed Nodes available with NSA application for Auditing.
2. From the complete list of licensed nodes you can select:
    - If any of these nodes matches, then trigger the rule
    - Only trigger this rule if certain required nodes match
3. When option 2 is selected, click the Correlate Nodes button.
4. The Set Correlation window opens.
5. Enter a Correlation Threshold value to establish correlation between Audit Scores of the selected nodes.
6. Select the node (s) to correlate.
7. Click **Save** to save the correlation settings, else click **Cancel** to abort the task.
8. The Rule is now configured and is ready to apply on the Policy.
9. Click **Save Rule** button.

Finalize Settings

Alerts can be set and managed by the user by configuring the fields to be considered from amongst the available fields such as Protocol, Source IP Address, Destination IP Address, Destination Port, Event ID, Virus Name, Attack ID and so on. Different Thresholds can be set for the events from configured nodes and when the thresholds are met within the selected time interval, an alert is triggered.

Threshold for the Rule

Users want to trigger alerts when a specific threshold is met within a specific period or when there arises a space complexity. The following are the options which can be used to finalize the threshold settings of the rule.

- Trigger this rule if it occurs at all.
- Trigger this rule if it occurs more than a specified value within specified period.
- Trigger this rule if it consumes more than - Kilo Bytes within specified period.

Application of Rules

Configured nodes at times generate massive amounts of data that can swamp security operators with false positives. Due to high amount of false positives there is a good chance of important malicious event being unnoticed or even if noticed, proper action could not be taken in time by the security personnel.

There comes the necessity of defining advanced correlation between alert triggering rules which help in triggering of alerts only when a combination of similar patterns across rules are satisfied among heterogeneous sources.

In NSA correlation can be specified using combination of:

- **Aggregate Fields**: port, protocol, Event ID, User Name, Source IP and Destination IP filters can be used as aggregate parameters.

For triggering of Individual Rule's within the policies there should be a unique combination of the Aggregate Fields which satisfies the *correlation value* set by the user.

After the settings are finalized, you can further use the logical operators And, Or to combine the rules and Not to negate the rules.

Alert Notification

An Alert if triggered is indication of an unwanted pattern/activity happening in the network. Administrator must be notified with these patterns in the form of alerts so that he can take corrective action in time. Following section provides insight of creating Alert delivery mechanisms in NSA. You can also import the Alert Delivery templates.

Alert Delivery

When an alert is generated, you can either choose to be notified by the following methods.

- Use Email Notification
- SNMP Trap Notification

E-mail

Select the E-mail check box for receiving alerts via e-mail. You can choose to not to include events in the generated alert. Also you can select to Include events in the body of the e-mail or to include events as attachment. The alert will have an HTML file as attachment with details of the generated alert.

Select any one of the options given below:

- Include Events as Attachment
- Do Not Include Events
- Include Events In Body

Leave the check box clear and the alerts notified through e-mail will contain only the time, alert name, alert description, and a message.

When Include Events as Attachment option is selected, you have the option to compress the events that are added to the email as attachment by selecting the Compress check box associated with the option.

Note: Alert messages can be configured to be sent in either HTML or Text formats.

SNMP Trap

SNMP (Simple Network Management Protocol) allows you to instantiate a trap-directed alert notification called the SNMP Trap. Trap-directed notification can help you save network and agent resources by eliminating the need for frivolous SNMP requests, and through minimized SNMP polling.

To configure NSA to send traps to the SNMP server, follow the steps described below:

1. Select the **SNMP Trap** check box.
2. Enter the appropriate details for the SNMP server IP/Name, SNMP Port, and Community Name.

Alert Recipients

On the E-mail Details panel you can set the time period, with in that if an alert is generated, it must be notified to a specific e-mail address.

Follow the steps described below to add a recipient:

1. Enter the time From to time To in the hh:mm format and the recipient's e-mail address. If an alert is generated within the specified time bounds, the alert message will be sent to the specified recipient.
2. Click the Add button. The e-mail ID is added to the recipient list.
3. Enter the subject and the message that should be passed on with the alert notification.
4. Enter the threshold value for alerts that you want to receive in an hour. For receiving e-mails, your SMTP server must have been configured.
5. To configure your SMTP server, click the Configure SMTP button. The Mail Preferences dialog box opens.
6. Specify the SMTP (Simple Mail Transfer Protocol) mail server name and user ID for NSA to send an e-mail alert whenever a specified event type or attack activity is detected or if the total number of attack attempts exceeds a specified value.
7. Finally, click **Save**.

Templates

NSA gives an option to create Alert Delivery templates, which can be used to notify intended recipients (admin users) for triggered alerts. You can directly import the settings defined in a template to any other Alert Delivery settings.

The Templates window displays the list of existing Alert Delivery templates on the Left pane and the corresponding synopsis for the template on the Right pane.

Set Permissions

Default Alert Policies:

Admin Users: By default all in-built polices are accessible to all Admin User accounts of the application. Any logged in admin user can Edit the settings of the policy, Save the settings to become the owner of the policy.

It is up to this Admin User discretion whether to allow other NSA users to View this Policy and able to Edit or Delete it or has the ability to Acknowledge, Clear the Alerts generated from this policy. After owning a Policy, this user can define access settings for other users using the Set User Permissions option present in the Create Policy window.

Non-admin users: The Power users have only Read-Only Permissions. Hence these policies are loaded to this user but cannot edit or modify anything.

User Defined Polices: If the user (admin or power users) creates a New Policy, then this user will automatically become the owner of the policy, this user can define access settings for other users using the permit other users using the Set User Permissions option present in the Create Policy window.

After owning a default policy or creating the new policy, you can set the permissions for other NSA users on this policy by clicking the Set User Permissions button. By default the User creating the policy will have All privileges on the Policy i.e., View, Edit, Delete, Acknowledge and Clear.

For example: If a power user creates the policy, this user will have All the privileges for the Policy. From the Set User Permissions window this power user can define the Access Settings (permissions) for other NSA users on this policy. When a user with View privileges tries to edit the Policy, following message is displayed.

When a user is granted the privilege to Delete a Policy, automatically all other Access Settings are also granted as to Delete a policy, other access (View, Edit, Acknowledge and Clear) should also be allowed for that user.

Summarizing the Permissions Scenario

User with:

- Read -> can view the policy settings as well as alert-archives
- Edit -> can change the filters (Read + Acknowledge + Clear)
- Delete -> can delete the policy (Read + Acknowledge + Clear + Edit + Delete)
- Acknowledge -> can acknowledge the alert-archive (Read + Acknowledge)
- Clear -> can view & delete the alert-archives (Read + Acknowledge + Clear)

Admin Alerts

Use the **Admin Alerts** screen to select the criterion on which you want to be alerted. To specify the criterion, follow the instructions given below:

Add Admin Alert

1. On the Alerts main screen, click the **New** button. The **New Admin Alert** window opens.
2. Enter the alert details (Alert Name and Alert Description) in the fields provided.
3. To specify the alert criteria, select any one of the following criterion:
    - Alert when an unknown node is detected.
    - Alert when free disk space NSA Server or Data Collector is less than user specified value. Specify the disk space limit in GB for Warning and Critical mail notification.
    - Alert when the devices (s) are inactive for more than the specified time.
    - Alert when the event count from the specified device (s) exceeds the specified number, every 5 mins.
    - Alert when user account is locked.
4. Select the nodes on which you want to generate admin alerts. Click **Next**.

    Note: If 'Alert when user account is locked' or 'Alert when an unknown node is detected' or 'Alert when free disk space is less than' option is selected, nodes selection is not required.

Alert Notification

1. Time Bounds: Enter the time From to time To in the hh:mm format. If an alert is generated within the specified time bounds, the alert message will be sent to the specified recipient.
2. E-mail address: Enter the e-mail address of the recipient in the text box. Click **Add** to add the mail recipient to the admin alert mailing-list.
3. You can configure admin alert to the same recipient at different time bounds or Click the **Clear** button to clear the e-mail address from the e-mail text box and add different e-mail recipients.
4. To delete a e-mail recipient from the list, select it and click on the Delete button.
5. Enter the subject and the message that should be passed on with the alert notification.
6. To configure your SMTP server, go to the E-mail dialog box in the **Options** tab. Click **Save**.
7. Click **Finish**.
   The newly created Admin Alert is populated on the main Admin Alerts window showing the details about Name, Description and Status in separate columns. You can enable/disable the status of the Admin Alert from here.

Edit Admin Alert

To edit admin alert, carry out the following steps.

1. Select the admin alert which you want to edit from the list.
2. From the menu buttons in the admin alerts window, click **Edit** button. The **Edit Admin Alert** window opens.
3. On the Edit Admin Alert window you can make the required changes in the alert notification criteria.
4. Click **Finish**.

Delete Admin Alert

To delete an admin alert, select an existing alert and click the **Delete** button available on the main screen of Admin Alerts. You are prompted for confirmation. Click **Yes** to confirm the deletion.

Alert Events

Once an Alert is triggered, the total count of events which meet the Policy settings are displayed in the Unacknowledged events column on the main Alert window. Here are the points entailing the use and scope of Alert events:

1. If the Alert has triggered, click on the count displayed in Unacknowledged Events column to open the Alert Events window.
2. The Alert Events window displays the Alert Name along with the associated list of Unacknowledged Archive in a timestamp format on the left pane.

Note: At any given time alert archive can show a maximum of 1000 recently triggered events.

3. Select a triggered Archived Event, the corresponding event details like – device type, device ID, Interface, Priority, event code, event type, event category are displayed on the right pane.
4. Click the **Acknowledge** button to acknowledge that particular event. The dialogue box prompts you to either Acknowledge or Acknowledge and Clear with every archived event you acknowledge the event count reduces simultaneously on the main Alert window.
5. Click the **Clear** button to acknowledge that particular event and also remove it from the list. With every archived event you clear the event count reduces simultaneously on the main Alert window.
6. Click the **Acknowledge All** button to acknowledge all the events. All the acknowledged events will be separately shown under the **Acknowledged Archive** list.
7. You can also opt to acknowledge and delete all the triggered events at one go, if you don't foresee any threat associated with the triggered alert by clicking on the **Clear All** button.

Note: Once you acknowledge an event it is removed from the alert archive list. You can go to App path ...Userprofiles\<user Name>\Alerts\<Selected Policy Name> to view acknowledged archives.

NOTE: You can access workbench from any event by double clicking on it.

Alert Archive

Once an Alert is triggered, NSA archives the event which is triggered last, based on the timestamp of the event. If there are more than one events triggered with the same timestamp, all are archived. Here are the points entailing the use and scope of Alert Archive:

1. If the Alert has triggered, click on the **Archive in Last Archive** column on the main Alert window to open the Alert Archive window.
2. The **Alert Archive** window displays last event (s) occurred in the Alert based on the timestamp of the event on the upper half of the window.
3. The details of the last event on the triggered alert like – device type, device ID, Interface, Priority, event code, event type, and event category and so on are displayed on the window.

NOTE: You can access workbench from any event by double clicking on it.

Chapter 19: Security Center

The Security Center button on the main GUI of the NSA, takes you to the Security Center, which comprises of the following modules:

Dashboard

NSA dashboards give a quick bird's eye view of your existing network infrastructure for deep analysis of security measures. By managing dashboards, you can track metrics, gain insight into the underlying security status by complete analysis of network components. Dashboard Manager provides a consistent and accurate way to monitor critical security areas.

Reports

This feature allows you to configure and generate reports. In addition to default reports that are non-editable, you can create custom reports tailored to meet your unique requirement. You can drill-down and obtain additional details for a selected top-level query.

Events

This feature allows you to monitor predefined criteria and giving insight into essential system events. You can create your own views to monitor recent viruses detected, attack detections, emergency events, alert events, warning events, average events per second, port activity, protocol activity, and more.

Security Center Options

You can launch the View option by Right-clicking on the Help icon. This option can be used to select the modules that are to be displayed in the security center. An admin user by default will have access to all the modules. For a Power user, View option will display only the permitted modules for that user. A report User will have only two options (Dashboard and Reports) from the View.

Select/Change the Security Center Options:

1. Right-click on the help icon displayed at the top-right hand corner of the Security Center window.
2. Select the **View** option.
3. The pop-up displaying all the Security center options is displayed.

4. A tick mark before the module name is an indication that it is already available in the Security center.
5. You can Select/De-select the Security Center options.
6. For the changes to take effect, close and revisit the Security Center tab.

Chapter 20: Dashboard

The Security Center button on the main GUI of the NSA, takes you to the Security Center, which comprises of the following modules:

Dashboard Manager delivers monitoring and reporting metrics—so authorized security personnel in the organization can monitor and understand the security posture of your network. Easy to build and user friendly, NSA dashboards give a quick birds view of your existing network infrastructure for deep analysis of security measures. By managing dashboards, you can track metrics, gain insight from underlying analysis, and can alter rules as conditions change. Dashboard Manager provides you with a consistent and accurate way to monitor critical security areas.

The default Dashboard screen comprises of various distinct panels that gives you an overview of following activity in your network:

- Event Viewer
- Top Sources
- Direction Chart
- Total Events
- Top Destinations
- Port Activity
- Top Attackers By Events By Victim
- Event Action Chart

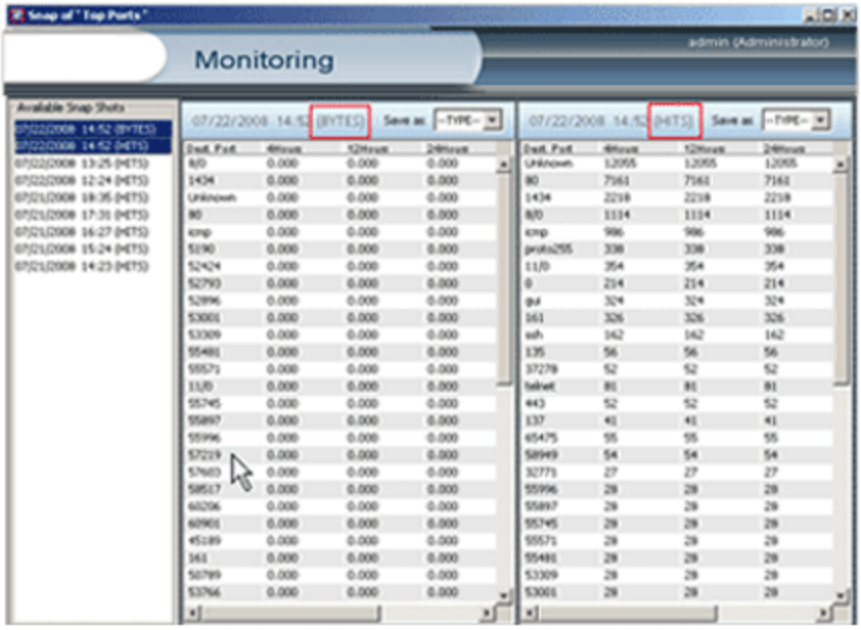
Design Options in Default Dashboard panels

There are two kinds of panels on the dashboard— Monitors and Reports. Each panel has the following options for reworking on the look and feel of the monitor. Click the icon in the dashboard panel, the following expandable list of options appear:

 **Zoom**: Use this option to maximize the current view.

 **Snap**: Use this option to capture a screen shot of the dashboard pane. NSA saves a copy of the snaps every one hour in a day, in chronological order. You can compare snaps taken at different times to evaluate the periodic status of the desired events on your Devices. Hold the ctrl key and select the time stamps of the snaps, the right pane displays the selected snaps adjacently, making it easy for you to track down the differences between them. You can simultaneously compare up to 12 snaps at one time.

Snapshot of the same monitor can be viewed in the following two ways:



Modify: Use this option to modify the information displayed on the pane.

1. Click on the icon, the **Modify Dashboard View** window opens.
2. There are two types of panel choices available to modify the Dashboard view that includes- **Monitors** and **Reports**.
3. If you want to modify the Dashboard by adding a Monitor, select Monitor or select Report radio button if you want to add a report or monitor view respectively.
4. On selection of the panel type, the corresponding list of queries id displayed. Select the required queries from the list that you want to view in the Dashboard.
5. Click **OK**.

This option is useful when you have to replace any of the dashboard panels with a new one without altering the placement of existing panels.

Drilldown: Use this option to delve into the information of the selected monitor. This is extremely useful when you want to generate a quick report and find out what contributed to the numbers present in the reports.

Table: Use this option to present the information of the selected monitor in a tabular format.

NOTE: If the number of Graph attributes for a monitor is more than twelve, its corresponding information cannot be shown in tabular format.

Graph: Use this option to present the information in different visual forms. You can opt to see the information in table and different graph types— Bar, Pie, Horizontal, Line, Radar and More. If you select more from the collapsible list of graph, the More Graph Types window

opens, where you can select from visually delightful various graph options like—Bar, 3DBar, Horizontal, 2DLine, 3DLine, PIE, 3DPIE, Radar, 2DArea, 3DArea.

Date Filter: If the selected monitor is a Report, you can apply Today, current Month or current Quarter filter from the dashboard panel.

Display Type: This option is made available if the data in the monitor can be displayed in tabular and graphical formats. You can opt to see the information as— Table, Bar, Tape, Pie, Horizontal, Area, Stock, Micro Bar and More.

Query By: Use this option to aggregate the data displayed in the report classified By Day or By Device or By Group or By Event Class.

View By: Use the **View By** option to generate monitor classified by Hits or Bytes.

Show Legend: Use this option to see Graph Legends, which are a key to the data plotted on the graph; on the dashboard panel.

Show Table: Use this option to see the information in a tabular form. The Show Table option is available on the graph monitors only. On selection of this option the table is shown below the graph.

Filters: If the dashboard monitor is Report, you can use this option to filter the data displayed in the monitor. Filters applied are specific to that Report (monitor) and do not effect other instances of 'same' report in any other dashboard.

Note: The 'Filters' option will be visible for only those report monitors which support 'Filters elements used in the Reporting Center'. Also the data in the report monitor should contain at least one column which can yield useful information upon filtering.

Customizing Dashboard View

With the choice to create personalized views, Dashboards are no longer exclusive to security administrators. As all role-based users need access to relevant security information in order to make right decisions. With Dashboard Manager, users can build personalized dashboards that give the information they need. Various personalization options make it easy to create custom dashboards for different users or groups of users.

The various options available under **Add/Edit a Dashboard** drop-down list are as follows:

New Dashboard- Use this option to create customized dashboards that allows you to view reports on desired information of all devices in a single view.

Copy Dashboard- If you want to instantly make a copy of the current dashboard, click on this icon, a dashboard pop-up comes up, prompting you to save the copy of the dashboard. By

default, the name of the copy of the dashboard is saved in Copy_of_<dashboard name> syntax. You can enter the name of your choice in the dialogue box and Click OK to save the copy of the dashboard.

Delete Dashboard- Network activity is dynamic in nature, therefore, what was required yesterday might become obsolete today. To keep pace with the changing information you can delete the unwanted dashboards by selecting this option.

Set as Default- If you have created a customized dashboard displaying information you need most and would want to monitor it regularly, then you can set that dashboard as the default view. Henceforth, the performance monitoring portal will open with the default view.

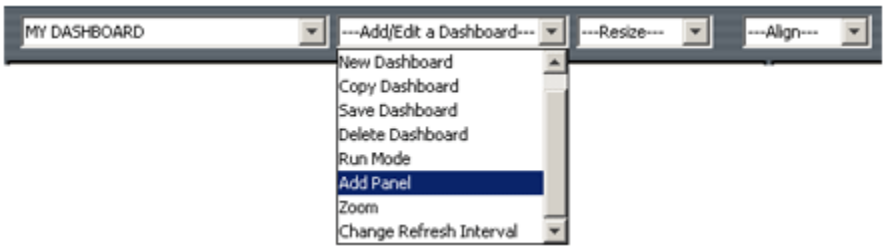
Restore Default- Use this option to restore the factory defined default view from the customized dashboard.

Zoom-Use this option to maximize and view the current dashboard in a new window.

Design Mode: NSA gives you extreme flexibility to change the look and feel of the customized dashboard. Open any customized dashboard that you have created and select this option to activate the design mode, and you can resize, drag and drop the individual monitors to arrive at a dashboard of your choice. The selection of this icon adds a few more tools that aid in designing a customized dashboard.

Note: If your current selection is the Default Dashboard, then this option will allow you to only resize or re-align the existing panels on the dashboard.

Tools to Edit Dashboard in Design Mode



Add Panel: If you want to instantly add a panel to the current dashboard, click on this icon, the add dashboard panel window opens. Select the desired queries for which who want to add a panel (s) to the current dashboard. You can opt to add device based panels of your choice to the dashboard.

Save Dashboard: Once you have redesigned your customized dashboard with chosen panels in desired size and position, you can save those settings by clicking on this icon.

Layout Design Tools: NSA provides easy-to-use, drop-down options to Resize and align the selected panels to create a desired layout on the dashboard.

Resize: Hold the ctrl key and select the panels that you want to resize. Following are resize options.

- Resize Width
- Resize Height
- Resize Both

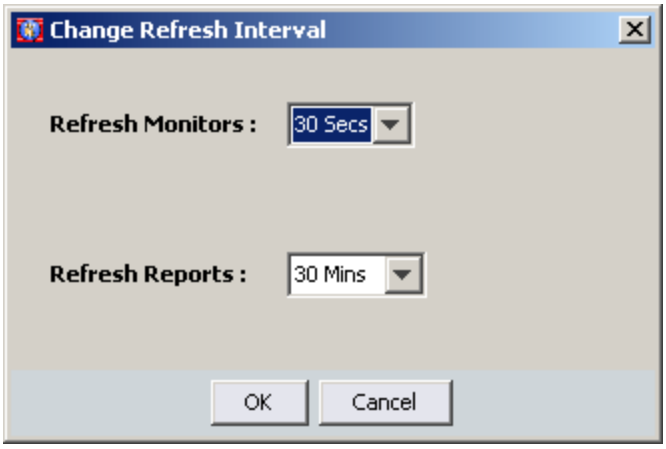
Select the panels that you want to set as a precedent in the end and select the desired option from the resize drop-down list. For example if you want to resize the width, select the desired panels and choose Resize Width option and all the selected panels width will be resized to the panel selected in the end. You can adjust multiple panels at a time by selecting them in succession by holding the ctrl Key.

Align: Hold the ctrl key and select the panels that you want to align. Select the panel that you want to set as a precedent in the end and select the desired option from the align drop-down list. Following are the options using which panels can be aligned.

- Left Align
- Right Align
- Top Align
- Bottom Align

Change Refresh Interval: Use this option to define the time interval based on which the data in the respective Report/Monitor panels will be refreshed.

Monitors: Select a time-interval from the Refresh Monitors drop-down list to set a frequency to refresh the monitoring data. You can refresh the data in monitors every 5, 10, 15, 20, 25, 30, 35, 40, 45, or 60 seconds. By default the monitors are refreshed every 30 seconds.



Reports: Select a time-interval from the Refresh Reports drop-down list to set a frequency to update the data in the Reports. You can refresh the Reports every 5, 10, 15, 20, 25, 30 or 60 minutes. By default the deltas are updated every 15 minutes.

NOTE: If your current selection is the default dashboard, then icon appears in a disabled state. You cannot resize or re-align the panels on the default dashboard, instead you can use task bar to modify the information displayed on the individual panels.

Jump to a panel of the Dashboard

NSA provides an easy way of locating specific dashboard panels when you have complex multi-panel dashboard view as locating a panel becomes difficult and time consuming.

Follow the steps to locate a panel:

1. Select the dashboard from the dashboard drop-down list.
2. All the panels of the dashboard are listed in the corresponding Panels drop-down.
3. Select a dashboard panel that you want to locate and view.
4. NSA automatically highlights and takes you there without scrolling or searching for the panel.

Add Dashboard Panel

NSA provides you the flexibility to add a panel to the current dashboard instantly. Follow the steps given below to add a new dashboard panel to the current customized dashboard:

1. Select the **Add Panel** option from the dashboard options in design mode, the add dashboard panel window opens.
2. Select the desired report or monitor for which you want to add a panel (s) to the current dashboard.
3. You can opt to add panels from - **Monitors** and **Reports** to the dashboard.
4. Click **OK**.

Create Dashboard

A dashboard is a user interface that organizes and presents complex information in a way that is easy to comprehend. NSA comes with an interactive, user friendly Dashboard comprising of viewing panes -- Real-Time Events, Event Graphs, Alert Graphs etc.

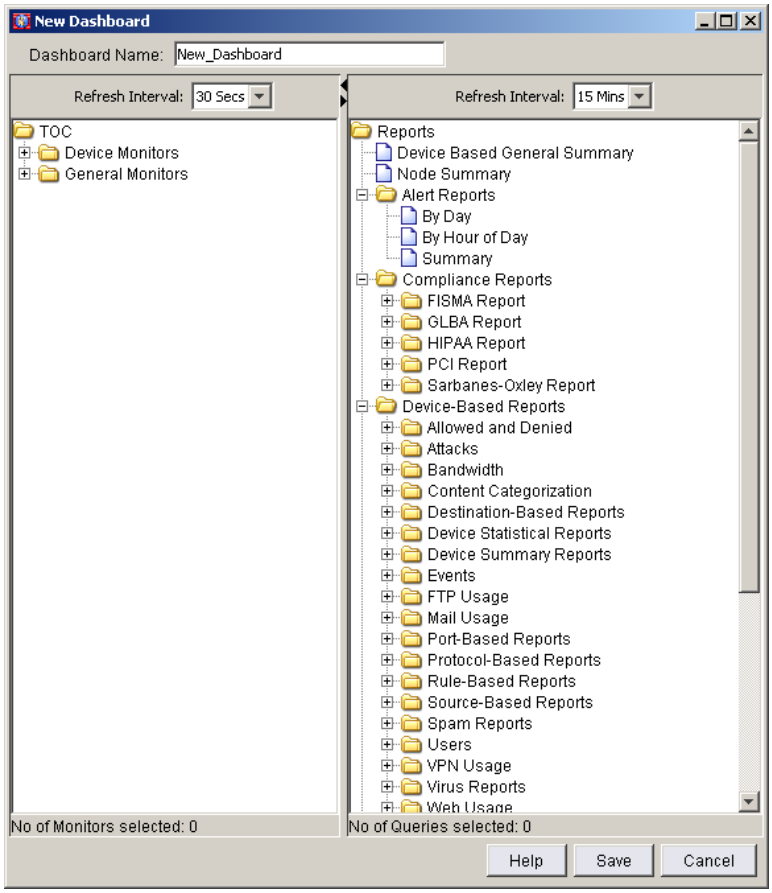
How to Manage?

On the dashboard main screen, the **Dashboards** drop-down lists containing all the dashboard views is available to the user.

To set a view as the default, select from the drop-down list and click the **Set as Default** option. To restore the default dashboard view, select the **Restore Default** option.

Creating New Dashboard

You can create customized dashboards to view the reports and monitors on desired information of devices at once.



Follow the steps given below to create a customized Dashboard:

1. On the dashboard options menu, select the new dashboard option. The create New Dashboard wizard opens.
2. Enter a Dashboard Name for your customized dashboard.
3. Select the Monitors and Reports that you want to be part of the dashboard.
4. Select the monitors you want to set in the dashboard view from the Monitoring TOC.
5. Select the query (s) to generate a report on the selected monitor from the Reports pane. Hold the ctrl key and select the reports to view in the dashboard, click **Save**. The created Dashboard is populated in the Dashboard drop-down list.
6. Click **Save**. The dashboard view is saved and listed in the dashboards drop-down list.

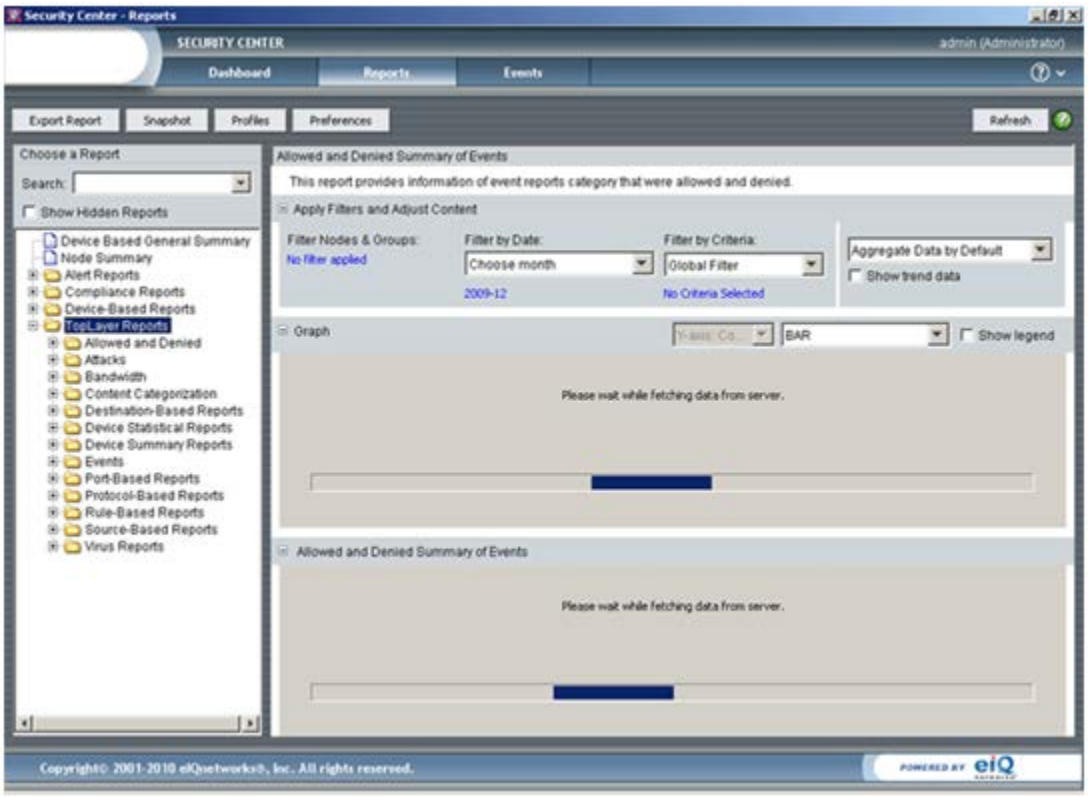
NOTE: By default, dashboard view is opened in the Run Mode. To change the mode to Design Mode, click the design mode option, resize or rearrange the monitors available on your dashboard view and then click on the mode icon to restore the run mode.

Chapter 21: Reports

The Reports Portal is the platform where you can create and generate a report to view a single query on the fly without creating a profile. This is helpful when you want to quickly view data for a single query. Access to the Security Center depends on the login privileges of the user. If you have logged in as a Power User or User, you are allowed to report on only those devices/reporting sections you have permissions for.

Click here for information on the types of users and privileges associated with each user type.

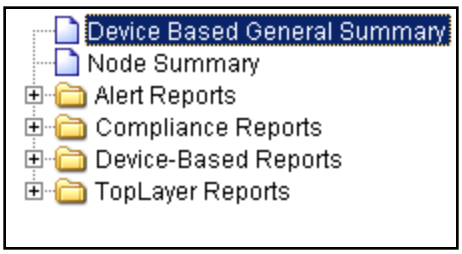
The Reports Portal



If you have logged in as a Power User or User account, you are allowed to report on only those devices/reporting sections you have permissions for.

Table of Contents Frame

The Table of Contents displays a list of the available Report Sections. To expand or collapse a Report Section, click the folder icon or '+' mark to the left of the Section name. Some Sections contain sub-Sections. Similarly, sub-sections can also be expanded and collapsed. Click the **Report Name** to view the report.



All the queries that come under a common category are grouped under a single section. Now, you can see all the related queries under the required category and can obtain more precise information from the log data. Some of report categories included are.

Some of report categories included are:

Device based reports: The reports under this category give a quick assessment of the devices in the network. It includes the Attack based reports; Event based Reports, Bandwidth Reports, and Web Usage.

Compliance Reports: NSA supports the documentation demands of the regulatory compliance acts. On the Compliance Report module of NSA, you can generate comprehensive reports on the events happening on the Devices in your network perimeter, to demonstrate and affirm the security of your network. Each industry domain is governed by a separate law; with NSA you can generate one-click reports supporting the following laws like:

- **HIPAA**: HIPAA regulations have widespread impact on healthcare providers and insurance companies. The regulations are complex and require significant documentation and reporting. NSA provides comprehensive reports to assist meeting the critical reporting requirements of the HIPAA regulations. The HIPAA reports include information on-Failed Login Attempts, Account-misuse, lockouts and deletion, changed passwords, ownership changes... to name a few.

- **GLBA**: The Gramm-Leach-Bliley Act (GLBA) has widespread impact on financial institutions including banks, mortgage brokers, lenders, credit unions, insurance and real-estate companies. The regulations are complex and require significant reporting on the processes in place that guarantee the integrity of customer data. With NSA you can generate reports to fulfill these requirements, the reports include information on-Failed Login Attempts, Account-misuse, lockouts and deletion, changed passwords, ownership changes... to name a few.

- **FISMA**: The Federal Information Security Management Act (FISMA), outlines requirements to secure Federal information. Each Federal Agency must develop, document, and implement an agency–wide information security program to be compliant with FISMA. NSA helps you to improve FISMA compliance by providing reporting capabilities on threat and network discovery thereby ensuring the enterprise security and be compliant with FISMA.

- **PCI**: The PCI (Payment Card Industry) data security standard compliance calls for total network security of the credit cards system environment, which includes thorough scanning of network activity at system, transaction and application level and produce the relevant evidence in the form of reports. NSA gives you an option to generate exclusive PCI reports which include information on Password Changes, Vulnerabilities list, Remote activity, Audit events, Log on- Log off activity, Account deletions...

- **SOX**: Sarbanes-Oxley act documents specific regulations required for publicly traded companies to document the Management's Assessment of Internal Controls over security processes. The overall requirements of the regulations can be summarized as: (1) documenting commitment to a process, (2) documenting the effectiveness of the process that's in place, and (3) documenting an auditor's assessment of the company's assessment of the process that's in place. To achieve the same, NSA provides reports on- Failed Login Attempts, Account-misuse, lockouts and deletion, changed passwords, ownership changes.

Statistical Reports: Comparison of different types of data like – Attacks versus Events over user defined time interval, between different protocols, etc. There are two types of statistical reports:

- **Hourly Statistics**: These are available for all "Hour of Day" reports. To obtain Hourly statistics, select Historical option in Query By of any Hour of day report. These reports show variation of count (hits or bytes) over 24 hours for the selected days with the hourly count (hits or bytes) of month currently under selection.
- **Daily Statistics**: These reports are available as a separate section of reports like Device Statistical reports. There are two kinds under these, Static and Dynamic.
  - **Static Daily statistic reports**: provide variation of count (hits or bytes) of 'quantities' over the selected days. These quantities depend on the report query under consideration. For Example, Attacks and Events Stats by Day shows variation of attacks and events over the selected days.
  - **Dynamic Daily statistic reports**: provide information about the variation of top ports and protocols (dynamically determined from the database) over the selected days. These are available as a subsection called Top Statistics under Device Statistical reports.

Summary Reports: Reports displaying consolidated data on Devices. For Example, a report displaying count of all types of events (virus/spam/alerts/attacks/etc.,) that took place on all the Devices within the Organization.

Distribution Reports: These reports display number of devices which are distributed over a range of count on attacks/virus events/spam events etc. For Example, user can identify the count of devices which fall under distribution range with highest activity/count/events.

Show Hidden Reports: By default some of the query sections are hidden as they are used rarely by the user. Select this option to view the hidden queries.

Note: For the Queries based on Hour of the day the number of Records is fixed to 24 and the number of Sub-records to 10, hence the customization of records option is not functional while generating a report based on these queries.

Report Frame

The report frame on the right hand-side of the screen displays either the report chosen in the table of contents for the time frame chosen in the calendar or the chosen dashboard. The default item to appear in the report frame is usually the dashboard for the default template.

Reporting Utility Options

In addition to the easy-to-use dashboard design tool bar, you can leverage on the simple reporting options to generate the desired reports. You can generate reports, showing only the mandatory data by applying the global filters. NSA provides the following options to — create, publish, and export profile based reports, apply global filters and convert the reports in desired formats. In the upper right-hand corner of the Reporting Portal, you can find the commonly used utility options of the reporting center. They are:

Export Reports: Click on this button to narrow down the scope of the report to show only the required information by picking up the related queries or templates. You can generate the customized report and export it to a desired format from here.

Snapshot: Use this option to capture a screen shot of the report in a new window.

Profiles: Click on the **Profiles** button to access the profile portal, where you can create profiles to generate exclusive reports with specific filters on specific devices, schedule them, assign unique style and save them at a specific location in the desired format.

Preferences: Click on this button to apply the DNS Lookup settings for the selected query or reporting section.

Additional options available on the reporting center:

Refresh: Click the **Refresh** button to show the current available data on the Reporting Window.

Close: The **Close** button closes the current window and exits the Reporting Portal.

Help: The Help icon brings up a Help window with additional information about the Reporting center.

Report Pane

The report frame on the right side of the Desktop displays either the report chosen from the Table of Contents for the time frame specified in the calendar. The default item to appear in the report frame is the device summary report. The displayed report consists of a title, the applied filters, a short description, and a table of results. Each report has a unique help card, displayed in the report. The help card contains information to help you interpret and make use of the information displayed in the report. In most reports, each graph is color-coded to relate items in the table to items in the graph if there are more results than can be displayed in the table or graph.

Apply Filters and Adjust Content

Filter Nodes and Groups

The tree starts with the default group and its affiliated Devices, followed by the hierarchic display of other customized groups and their affiliated Devices. If you do not create any groups, then the Device tree shows only the default group along with its associated Devices.

If you want to restrict your information in Reports only to a particular device, then use this option by clicking the hyperlinked text to bring up the Groups tree.

Select the Device followed by the desired Report, the output displays only the data pertaining to the selected device.

Filter by Date

You can use this option to apply time filters across the available reports. Various filter options facilitate selection of following time periods.

- Today
- Yesterday
- Choose a date range
- Choose Week
- Choose Month
- Choose Year
- Quarterly

With the Choose Month option you can change the month that appears in the Calendar for any given year. When you choose a date range, specify the Start Date and End Date. For Choose Week options, along the right-hand side of the calendar are the Select Week buttons. Clicking one of these buttons selects the corresponding week. There are Month, Quarterly, or Year icons along the bottom of the calendar depicting respective selection from the filter options.

You cannot view the aggregated data in the report if View quarter or View year date filters from calendar are applied.

NSA Regional Server: When using Month, Quarterly, or Year filters on the regional server database, make sure that the following flag is set in the <Your path>/Corero Network Security Analyzer/CoreroNSA/fwaconfig.ext file for performance reasons.

Regionalgrouping=yes

Note: If this flag is not set, performance of regional server is degraded and report generation will consume more time and resources.

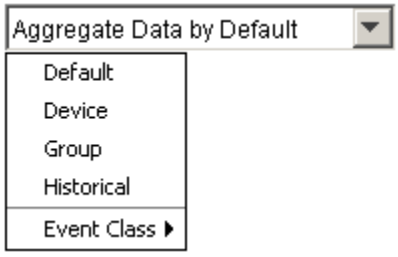
Filter By Criteria

The filter expressions applied to the instant report are shown under the Report title, they can be any one or all listed below, depending on the filters applied on the report:

- **Global Filter**: This link opens a pop-up window to show the Global Filters applied on the instant report being displayed. The Global filters take precedence over the Local filters in the report and are considered first.
- **Local Filters**: This link opens a pop-up window to show the filters which were applied locally from the instant report.

Aggregate Data by

You can classify on how the data in report should be aggregated and displayed. Use the Aggregate Data by drop-down list to specify the report classified By Day or By Device or By Group or By Event Class. You can also see the Historical reports for Hour of Day queries. Please note that some queries are classified only by device. If you have created an Event Class to bring together a set of events containing common variable (s) through a Policy, you can Query by that Event Class and generate a report on the same from the reports portal.



Note:
- The Event Classes created in the Policies module are subsequently populated in the Query By drop down list on the reporting center and an exclusive report can be generated on the selected Event Class.
- Query By Day/Device/Group option cannot be applied in conjunction with View Quarter or View Year date filters from calendar.

Historical: Selecting the Query By > Historical option to view the historical report of any Hour of Day query in the Security Center. By selecting this option, Historical column is appended in the report of all hour of day queries. In a Historical report, the average and per hour count for the selected days are plotted against the total per hour count for the entire month**.**

Include Trends: Use this option to record the trend of specific current and previous events happening at the devices.

This helps in determining the number of times a particular event type occurred over a period of time. The report will append the following columns displaying information about the event count to judge the event trend:

- Today's Count
- Yesterday's Count
- Last Seven Days
- Current Month

Graphs

Hide Graph: By default the Reporting Pane is divided into two horizontal halves. The Graph type Report is displayed on the upper half and the table type Report is displayed on the lower half of the Reporting Pane. Click on the '-' mark to hide the Graph and get a better view of the associated tabular report**.**

Graph Criteria: You can select to view the graphs based on event count or by bytes transferred for each query selected on the Y-axis.

- Y-axis-Count
- Y-axis-Bytes

Most of the queries support only the count criteria. Queries based on Data transfer support both Count and Bytes graph criteria.

Graph Type: By default the graph type displayed is the BAR graph. The type of graph is dependent on the kind of data available for that Query. You can select to view the graph type in the following formats:

- BAR

- PIE
- TAPE
- HORIZONTAL
- AREA
- STACKED HORIZONTAL
- STACKED VERTICAL
- MORE

Graph Legends, which are a key to the data plotted on the graph are shown on the reporting center depending on the graph type and associated number of records. For Pie-charts, the graph legend is shown on the reporting center only if the numbers of records present in the selected query are not more than 24. Whereas for other graph types the graph legend is shown only if the number of entries of data elements related to the selected query are not more than 12.

For single row data, only line graph will be displayed irrespective of the graph option selected.

Reading a Report

All reports consist of a title, a short description, and a table of results. In most reports, each graph is color-coded to relate items in the table to items in the graph if there are more results than can be displayed in the table or graph. Each report has a unique help card, displayed in the report. The help card contains information to help you interpret and make use of the information displayed in the report.

Drill down

Instant Reports provide the ability to drill down into a report to obtain further details. This is extremely useful when you want to study the behavior of a specific user or find out what contributed to the numbers present in the reports.

How to drill-down?

Right click on the values in the table to open the Workbench view for the instant report. Select the attribute (s) for which you want to narrow your scope to excavate finer details, click the Apply Filter button and resultant information based on your selection is displayed in a different window.

Quick Launch Options

If you want to instantly drill-down on a Device listed in the tree, use the quick launch options. Right click on the Device. A pop up displaying the following Quick Launch Options comes up:

- View Events
- View Stats
- View Collection Stats
- Reporting Drilldown
- QuickVue

- Workbench

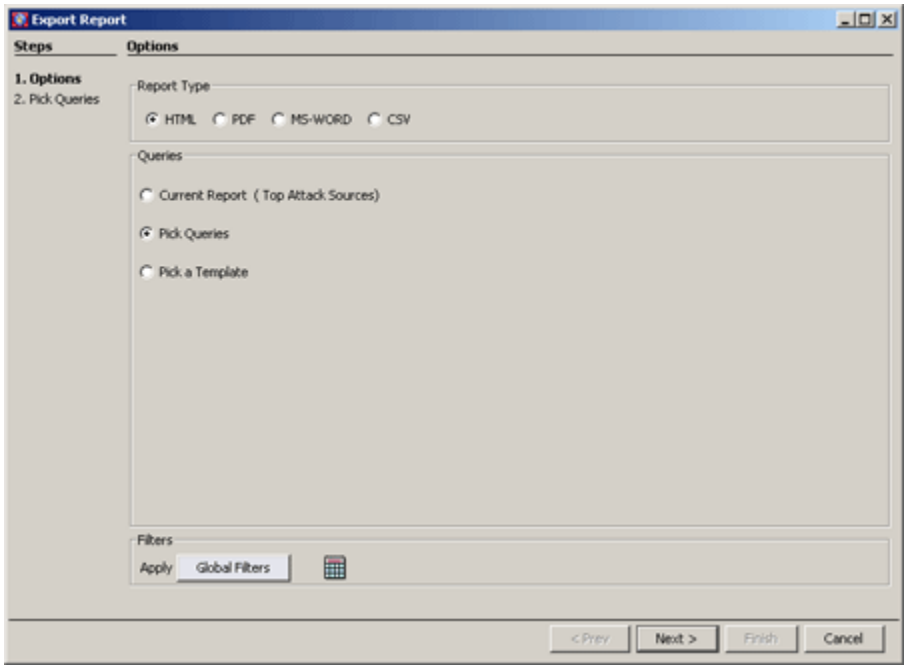
Click on the quick launch option to view more details about it.

Export Report

To export a report, select the queries and a rendering format from the available options and click Generate Report. The report based on the selected queries is generated and it subsequently opens in the application associated with the format rendered. For example, choosing PDF opens the report in Adobe Acrobat Reader.

Follow the steps described below to export a report by selecting the queries to report on:

1. Click **Export Report** from the main window. The Export Report window opens.



2. **Report Type**: The selected reports can be exported to HTML, PDF, MS-Word or CSV formats.
   Internet browser settings for opening different formats of Reports after you export them:
   PDF/MS-Word reports: Go to **Internet Options > Advanced Settings > Security** and leave the check box **Do not save encrypted pages to disk clear** for the PDF reports to open upon exporting them.
   MS-Word reports: Go to **Internet Options > Security > Security Settings**. Click on the Custom Level Button and **Enable** the "**Automatic prompting for File Downloads**" under **Downloads** as shown in the image below:
3. Use any one of the following options to narrow down the information that you need in the exported report:

- Current Report: Select this option when you want to export the Query that is currently selected in the reporting portal.
- Pick Queries: Select this option when you want to specific queries to export from the list of all the reporting sections available in the application and their corresponding queries. Click Next. Select one or multiple queries to generate a report on.
- Use Templates: Select this option when you want to export reports that are bundled with the application as templates. Click Next. Select a template to generate a report on.

4. Filters: Click on the **Apply Global Filters** button. The Global Filters window opens. Define the filters to be applied in the reports.

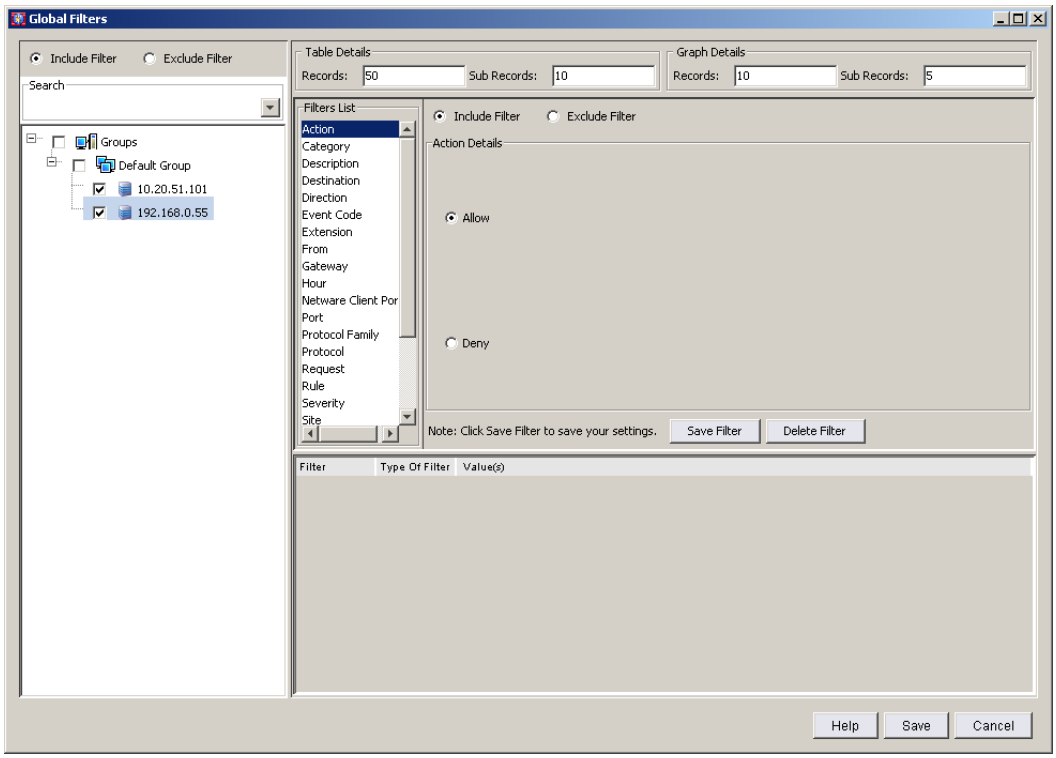
   Note: You can apply Global Filters from the main reporting window also.
5. Click **Finish**, a comprehensive report is compiled based on all the selected queries and is exported to the specified format.

Global Filters

Global Filters can be used to apply filters uniformly across the selected queries and are also available on the Export Report window. The filters will be applied to the reports, which are to be exported either to HTML, PDF or MS-Word formats. You can narrow down the scope of report; specify the number of records to be displayed in the report by applying these filters.

Follow the steps below to configure Filter settings.

1. Click on the **Global Filters** button from the Reporting Portal or from the **Export Report** window. The Global Filters window is displayed.
2. By default, the Global Filters window displays all the devices in the left pane. Select the devices to apply filters.
3. Specify under **Table** and **Graph** details, **Number of Records** and **Number of Sub Records** to be displayed in the report output.
4. By default NSA lists **All** the filter entities on which you can narrow your scope.
5. You can also enlist the filters based on Devices:
   - Device based Filters
6. To save the applied filter settings, click **Save**.



Device Based Filters

Filter Name	Column ID	Description
Action	act	events/attacks (Device) Has only two values (allow, deny)
Category	cat	Device Category filter
Source	cli	Device Client (Source) filter
Description	desc	Description filter
Direction	dir	Bound filter for device (Has two values - In, Out)
Destination	dst	Device Destination filter
To	dstemail	Destination email (To) filter for Firewall Devices
Event Code	ec	Event Code Filter
Extension	ext	Extension filter (Device Virus)
Protocol Family	family	Protocol Family filter (Device)
Gateway	gw	GateWay filter (VPN)
Hour	hod	Hour of Day filter
Port	port	Port filter
Protocol	pr	Protocol filter
Severity	pri	Severity filter for Device(Emergency(0) - Debug(7))
Request	req	Request filter
Rule	rule	Rule filter (Device)
Description	shortdesc	Short Description filter
Site	site	Site Filter (Web)
From	srcemail	Source Email (From) filter (Device)
User Name	user	User Filter (User Name)
Virus Category	vcat	Virus Category filter (Device)
Virus Name	virus	Virus Name Filter

Filters

Use Filters to narrow down the scope of the report, increase the number of records displayed, and change the graph type. The sections of the filter vary depending on the selected report.

Follow the steps below to configure filter settings.

1. Select a Report query from the list displayed on the left pane, click on the filter icon on the right pane and the corresponding Filters window is displayed.
2. On this window, you can select the devices you want to report on and the filters that can be applied for the selected query.
3. Similarly all the queries have corresponding filters to generate custom reports.

NOTE: Not all reports are associated with graphs.

Report Options

Use the report Options to change the DNS settings and logged in non-admin user password settings.

The DNS Lookup settings affect the reports that display IP address. The default setting is not to resolve IP addresses. The second option is to always resolve IP addresses into fully qualified host names by looking up values from the local DNS server. The third option is to perform the IP resolution from DNS cache that is in-built. For performance reasons, this is the recommended setting if DNS resolution is needed.

NOTE: Since the results from DNS resolution are not stored in the database, you will not find any resolved names when applying a host name filter or any other filter on the resolved IP addresses.

The Change Password option is available only for Non-Admin and Non-Power users and it allows them to change their login password. An admin/power user can change the password on User Manager-> Edit User. A User with only reporting privileges can change his password details from Options window.

NOTE: If a non-admin and Non-power user does not have privileges to Reporting module, option of changing the password is available by clicking on the icon of the modules which the user has privileged to.

Follow the steps described below to define a new password:

1. Select the **Change Password** check box. The new password field is enabled.
2. Enter a new password for the user currently logged in.

3. Click **Set Options**.

NOTE: Make sure you provide the same password when you login into the application next time.

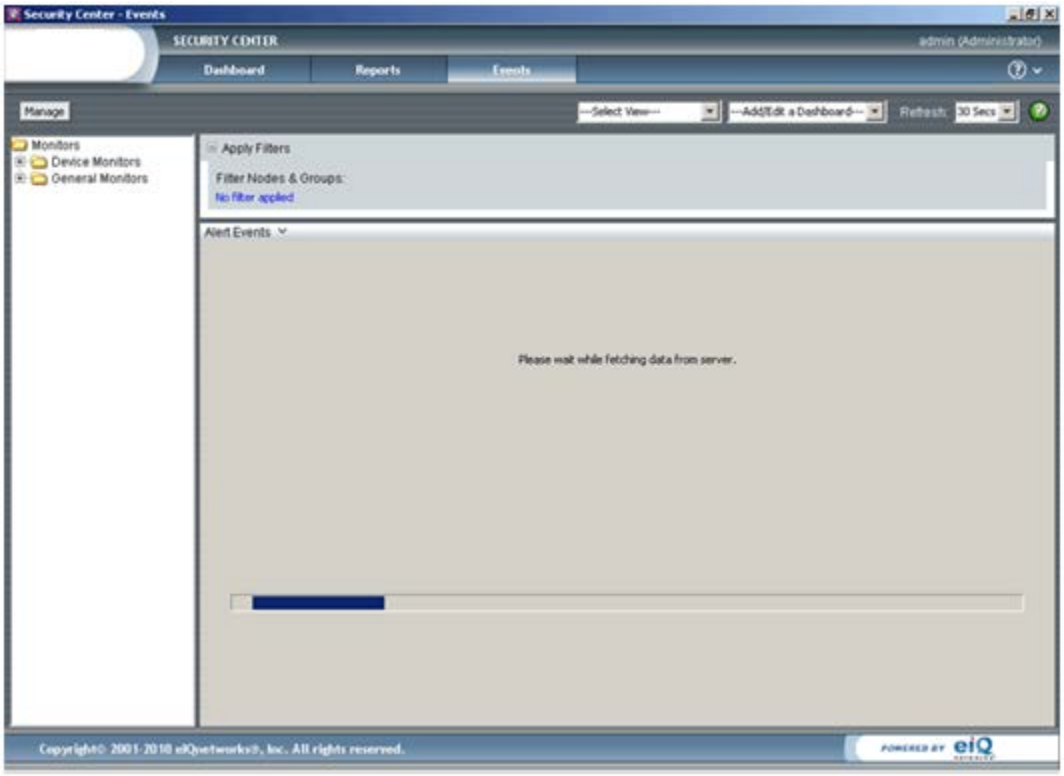
Profiles

Profiles: Click on the Profiles button to access the profile portal, where you can create profiles to generate exclusive reports with specific filters on specific devices, schedule them, assign unique style and save them at a specific location in the desired format. Click here for more details.

Chapter 22: Events

The Events feature of NSA facilitates monitoring on predefined criteria. This gives you an insight into the essential system events. You can also set filters on some predefined performance metrics and proactively deal with the enterprise security issues.

The Events module is the platform where you can monitor activities happening on all the Devices. You can also monitor the status of various policies configured on NSA for security and event management.



On the TOC pane of the Events platform, you can see the list of default and user-defined monitors. Select a monitor from the list and click on it to see its corresponding details.

Events -Task Bar

The task bar on the Events module contains the following icons to facilitate the respective tasks:

Manage - Use this button to create and manage new monitors based on devices.

New dashboard- Use this tool to create customized dashboards to view the desired monitors in a single view.

To Set as Default- You can use this tool set a custom dashboard as the default view, displaying information you need most and would want to monitor it regularly. Henceforth, the Events module will open with the default view.

Restore Default- Use this tool to restore the factory defined default view.

Copy dashboard- If you want to instantly make a copy of the current dashboard, click on this icon, a dashboard pop-up comes up, prompting you to save the copy of the dashboard. By default, the name of the copy of the dashboard is saved in Copy_of_<dashboard name> syntax. You can enter the name of your choice in the dialogue box and Click **OK** to save the copy of the dashboard.

Design/Run Mode- NSA gives you extreme flexibility to change the look and feel of the customized dashboard. Open any customized dashboard that you have created and click this toggle button to activate the design mode, and you can resize, drag and drop the individual monitors to arrive at a dashboard of your choice. The selection of this icon brings up the following tools that aid in designing a customized dashboard:

- **Add Panel**: If you want to instantly add a panel to the current dashboard, click on this icon, the add dashboard panel window opens. Select the desired queries for which you want to add a panel (s) to the current dashboard. You can opt to add both device based and host based panels of your choice to the dashboard.
- **Save Dashboard**: Once you have redesigned your customized dashboard with chosen panels in desired size and position, you can save those settings by clicking on this icon.
- **Delete Dashboard**: Network activity is dynamic in nature, therefore, what was required yesterday might become obsolete today. To keep pace with the changing information you can delete the unwanted dashboards by clicking on this icon.
- **Layout Design Tools**: NSA provides easy-to-use, drop-down options to Resize and Align the selected panels to create a desired layout on the dashboard.
- **Resize**: Hold the ctrl key and select the panels that you want to resize. Following are resizing options.

    - Resize width
    - Resize Height
    - Resize Both

- Select the panel, that you want to set as a precedent in the end and select the desired option from the resize drop-down list. For example if you want to resize the width, select the desired panels and choose Resize Width option and all the selected panels width will be resized to the panel selected in the end. You can adjust multiple panels at a time by selecting them in succession by holding the ctrl Key.

- **Align**: Hold the ctrl key and select the panels that you want to align. Select the panel that you want to set as a precedent in the end and

select the desired option from the align drop-down list. Following are the options using which panels can be aligned.

- Left Align
- Right Align
- Top Align
- Bottom Align

Note: You cannot resize or re-align the panels on the default dashboard in the run mode, instead you can use task bar to modify the information displayed on the individual panels.

Refresh: Use this option to define the time interval based on which the data in the Monitor panels will be refreshed. Select a time-interval from the Refresh drop-down list to set a frequency to refresh the monitoring data. You can refresh the data in monitors every 30, 60, 90 seconds or every 2, 3, 4, 5, 10, 15, 30, 45, or 60 minutes. By default the monitors are refreshed every 30 seconds.

NOTE: Enable the Monitoring option from the Collection Policy window to view events in the event viewer and the data displayed in the event viewer depends on the filters applied.

Quick Launch Options

If you want to instantly drill-down on an event on the event-viewer, use the quick launch options. Right-click on any event, a pop up displaying the following Right-click Options comes up:

- View Events
- View Stats
- View Collection Stats
- Drilldown
- QuickVue
- Workbench

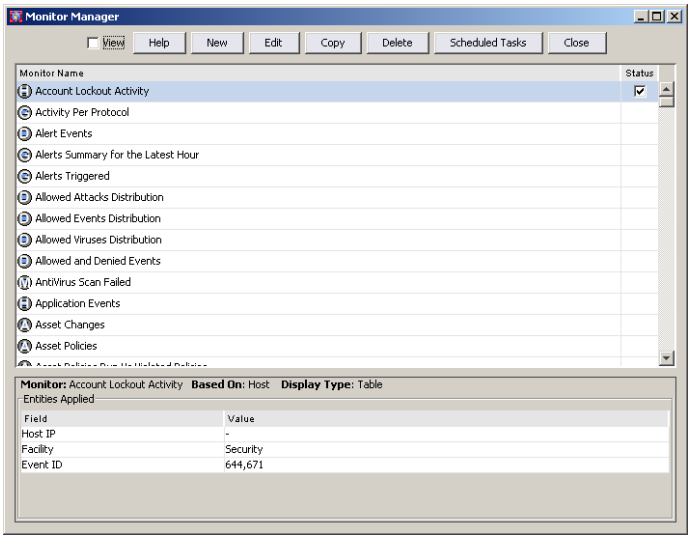
Click on the quick launch option to view more details about it.

Monitoring TOC

The 'table of contents' contain the list of monitors available in the Events module. Each topic has many sub-topics under it and you can select any to view its corresponding details. You can also add and configure a new monitor, by clicking the Manage button from the main menu of monitoring center. The Monitor Manager screen opens from where you can add new monitors based on the selected criteria.

Monitor Manager

This section provides instructions on how to add a monitor.

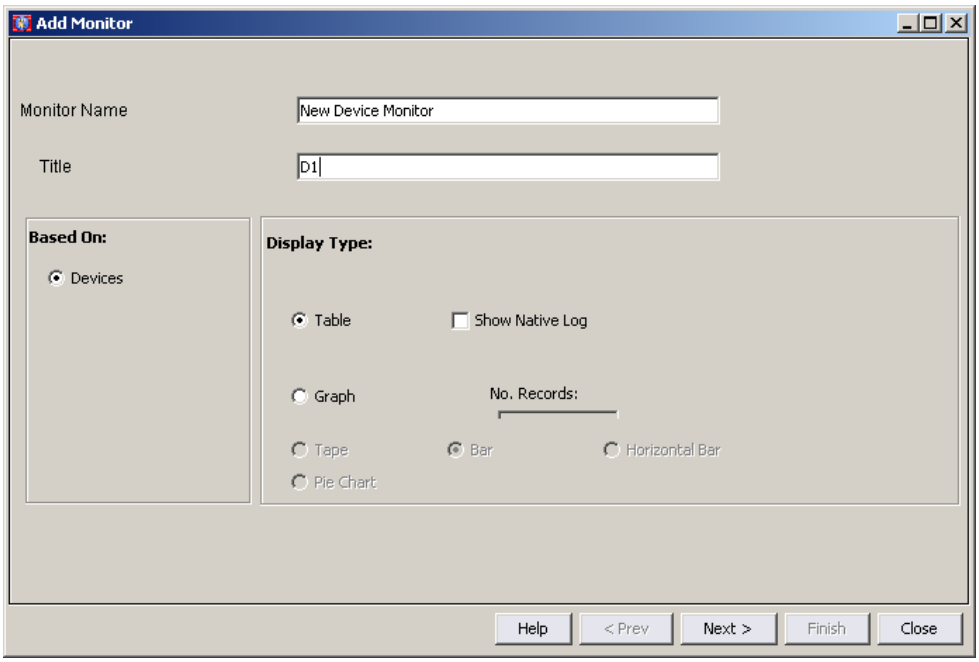


NOTE: Data from the entities to be monitored can be enabled or disabled by checking the corresponding status button.

The Add Monitor Wizard

Follow the steps described below to add a monitor:

1. From the Security Center main menu, click **Events**. The Events module opens.
2. Click **Manage** button. The Monitor Manager window opens. Click **New**.
3. Enter a name for the monitor in the Monitor Name box.
4. Enter a title for the monitor in the Title box.
5. In the add monitor screen you can select the type of monitor you are about to add/define. You can add a monitor based on any one of the following criteria:
    - Devices
6. There are two ways displaying information in the monitor. They are
    - Table
    - Graph
7. To customize the view, under the section Display Type, specify the graph type and number of graph items to associate with it.
8. Click **Next**.



Pie charts can be generated only if the monitor is created for a single entity.

Selecting Entities to Monitor

To select the entities to monitor, follow the steps described below:

1. Based on your selection, corresponding entities will be seen for devices. Select the entities you want to monitor from the list of available entity types.
2. Click on >> to move the entities into the list of selected entities.
3. Click **Next**.

If all the available entities are selected, the monitor does not display any information even if any of one of the selected entity does not have data.

Selecting Device Based Entities

NSA provides a comprehensive list of event entities that can be selected to be viewed in the monitors. They are:

- Action
- Event Class
- Event Description
- Attack Details
- Virus Details
- Spam Destination Email
- Spam Source Email
- Bytes Sent
- Bytes Received

- Shun
- User Name

Definable Event Entities:

In the logs, the value of some event entities may vary in different events depending on the external or internal factors. You can specify a desired value or parameter and restrict the monitor and view only those events that satisfy the specified value or parameter of the entity. The following filters can be defined with a specific value or parameter from the UI:

- Destination IP
- Destination Port
- Event Id
- Event Type
- Flow
- Protocol
- Rule
- Severity
- Source IP
- Spam Type
- Virus
- Device IP
- Attacks

Click on the filter to see the steps specific to each one of them

Device Based Entities

The following sections explain how to select device-based entities to monitor.

Source IP

If you have selected Source IP, follow the steps described below:

1. Enter the client IP you want to monitor.
2. To monitor events from a series of devices at one time, select the **Range** check box and enter the IP Range.
3. Click **Add** to add the client IP or range and click **Save Filter** to save the filter settings.

Device IP

You can select the Group Name/Device IP - Device Type for which you want to create a monitor.

1. Select the devices you want to create a monitor for. You can select all devices at a time or individual groups and devices.
2. Click **Next** for defining more filters else **Close** to exit.

Destination IP

If you have selected Destination IP, follow the steps described below:

1. Enter the Destination IP of the device you want to monitor.

2. To monitor events from a series of devices at a time, select the Range check box and enter the IP Range.
3. Click **Add** to transfer them in the Entered Values.
4. Click **Save Filter** to save the filter settings.

Destination Port

If you have selected Destination Port, follow the steps described below:

1. Enter the destination port number you want to monitor.
2. Click **Add** to add the port number to the list.
3. Click **Save Filter** to save the filter settings.

Protocol

If you have selected Protocol, follow the steps described below:

1. Enter the protocol you want to monitor.
2. Click **Add** to add the protocol to the list.
3. Click **Save Filter** to save the filter settings.

Severity

If you have selected Severity, follow the steps described below:

1. Select the priority you want to associate with the monitor from the Available Severities -- Emergency, Error, Critical, Alert and Warning.
2. Click  to transfer the selected priorities to the Selected Severity list.
3. Click **Save Filter** to save the filter settings.

Virus

If you have selected Virus, follow the steps described below:

1. Enter the virus name you want to associate with this monitor.
2. Click **Add** to add the virus to the list.
3. Click **Save Filter** to save the filter settings.

Attacks

If you have selected Attacks, follow the steps described below:

1. Select the attacks you want to associate with the monitor from the Available Attack list.
2. Click  to transfer the selected attack types to the Selected Attacks list.
3. Click **Save Filter** to save the filter settings.

Event ID

If you have selected Event ID, follow the steps described below:

1. Enter the event ID you want to monitor.

2. Click **Add** to add the event ID to the list.
3. Click **Save Filter** to save the filter settings.

Event Type

If you have selected Event Types, follow the steps described below:

1. Select the Event Types you want to associate with the monitor from the Available Event Types list.
2. Click  to transfer the event types to the Selected Event Types list.
3. Click **Save Filter** to save the filter settings.

Rule

If you have selected Rule, follow the steps described below:

1. Select the rules that you want to monitor from the list.
2. Click **Save Filter** to save the filter settings.

Flow

If you have selected Flow, follow the steps described below:

1. Select from the following
    - Inbound
    - Outbound
2. Select Inbound if you want to monitor only incoming events.
3. Select Outbound if you want monitor only outgoing events.
4. Click **Save Filter** to save the filter settings.

Spam Type

If you have selected Spam, follow the steps described below:

1. Select the Spam types you want to monitor from the predefined spam list.
2. Click  to transfer the Spam types to the Selected Spam Type list.
3. Click **Save Filter** to save the filter settings.

Events Dashboards

The Events Module is equipped with some very useful factory made dashboards, they are:

- All Events View
- Attacks View
- Bandwidth Info
- Bytes Info
- Client Info
- Default Dashboard
- Events Activity
- Events Distribution View
- Event Viewer View

- Misc View
- Ports
- Protocol View
- Source Activity View
- Virus Info

New Dashboard

You can create customized dashboards to view the monitors on desired information of Devices and Applications. Follow the steps given below to create a customized Dashboard:

1. On the dashboard options menu, select New Dashboard option. The create New Dashboard wizard opens.
2. Enter a Dashboard Name for your customized dashboard.
3. Select the monitors you want to set in the dashboard view from the Monitoring TOC.
4. Hold the ctrl key and select the reports to view in the dashboard, click **Save**. The created dashboard is populated in the drop-down list.
5. Click **Save**. The dashboard view is saved and listed in the dashboards drop-down list.

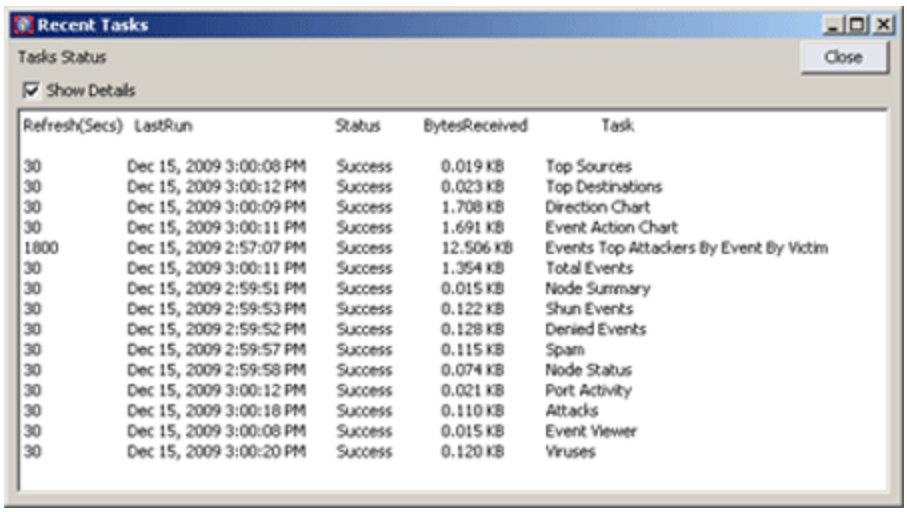
Add Dashboard Panel

NSA provides you the flexibility to add a panel to the current dashboard instantly. Follow the steps given below to add a new dashboard panel to the current customized dashboard:

1. Select **Add Panel** option from the drop-down menu, the **Add Dashboard Panel** window opens.
2. Select the desired dashboard for which you want to add a panel (s) to the current dashboard.
3. You can opt to add panels from the list of all available monitors.
4. Click **OK**.

Scheduled Tasks

The monitor is refreshed as per the Refresh Interval set on the Dashboard portal. Click on the **Scheduled Tasks** button available in the **Manage ->Monitor Manager** window to know the last run time for each monitor shown in the dashboard. The following screen is displayed.


Recent Tasks
Tasks Status
Close
Show Details
Refresh(Secs) LastRun Status BytesReceived Task
30 Dec 15, 2009 3:00:08 PM Success 0.019 KB Top Sources
30 Dec 15, 2009 3:00:12 PM Success 0.023 KB Top Destinations
30 Dec 15, 2009 3:00:09 PM Success 1.708 KB Direction Chart
30 Dec 15, 2009 3:00:11 PM Success 1.691 KB Event Action Chart
1800 Dec 15, 2009 2:57:07 PM Success 12.506 KB Events Top Attackers By Event By Victim
30 Dec 15, 2009 3:00:11 PM Success 1.354 KB Total Events
30 Dec 15, 2009 2:59:51 PM Success 0.015 KB Node Summary
30 Dec 15, 2009 2:59:53 PM Success 0.122 KB Shun Events
30 Dec 15, 2009 2:59:52 PM Success 0.128 KB Denied Events
30 Dec 15, 2009 2:59:57 PM Success 0.115 KB Spam
30 Dec 15, 2009 2:59:58 PM Success 0.074 KB Node Status
30 Dec 15, 2009 3:00:12 PM Success 0.021 KB Port Activity
30 Dec 15, 2009 3:00:18 PM Success 0.110 KB Attacks
30 Dec 15, 2009 3:00:08 PM Success 0.015 KB Event Viewer
30 Dec 15, 2009 3:00:20 PM Success 0.120 KB Viruses

Chapter 23: Right-click Options

The activity on the network components is dynamic in nature. The events happen faster than one can imagine. Due attention should be given to events as it can potentially lead to major security issues. The details of the event may go unnoticed due to the high speed at which they occur. The Monitors, Reports and Event-Viewer on the NSA portals display information on the events occurring at the configured Devices. However, if you want to instantly drill-down on an event to excavate these details, use the quick launch options. Right-click on any event/node a pop up is launched displaying the Options available for that event/node.

NOTE: The quick launch options are dependent on the context from which they are launched. For example, Open Shell is available only on the main Device window; Run Command is available only on the Devices.

Add To Group

Use this option if you want to instantly add a Device under an existing or new Group.

Follow the steps given below to add a device to group:

1. Right-click on the node that is to be added under a group.
2. Select the **Add to Group** option.
3. All the existing groups in the Groups tab are displayed in the menu bar other than the default group.
4. Select a group to which you want to include the Device.
5. Alternately you can create a New Group and include the Device in it.

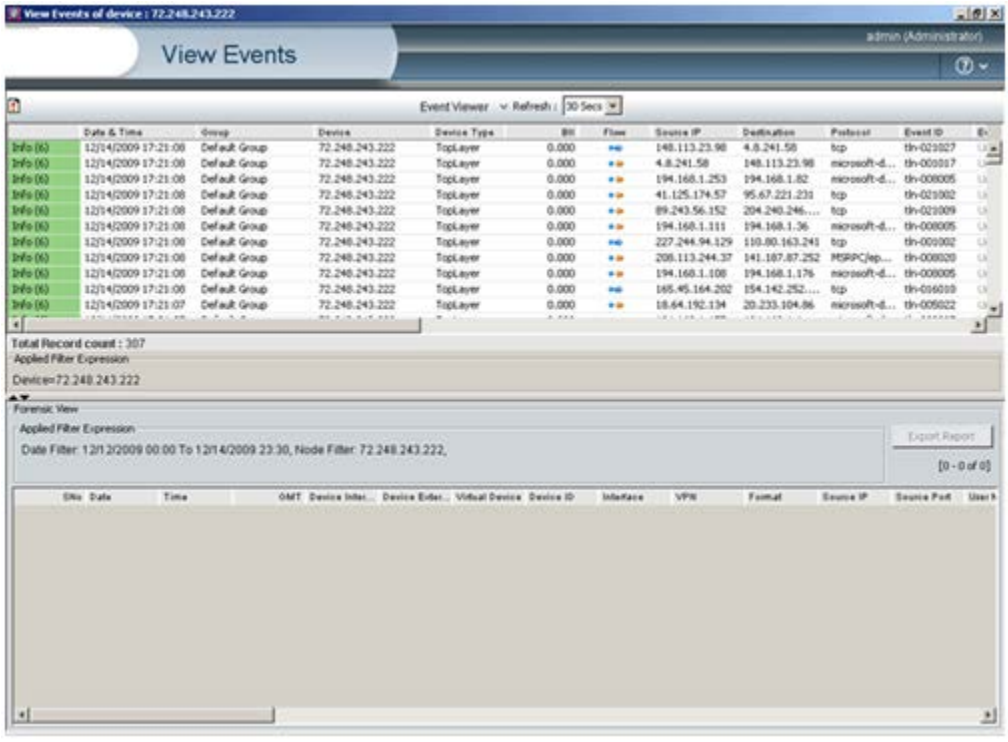
View Events

Real-time monitoring of your network components can help you take corrective actions in time to protect your network perimeter from attacks and misuse. It is important to have a continuous surveillance platform to monitor the real-time events which are ubiquitously accessible from anywhere in the application. To accomplish this, NSA provides View Events option in the Quick launch options. In addition to the real time monitoring, the bottom pane of the View Events window displays the Forensic view. The forensic view displays the Forensic data recorded in last three days on the filtered node.

Follow the steps given below View Events of the source selected:

1. Right-Click on the selected event, the list pops-up with Options. Select the **View Events** option from the list.

2. If you select an event originating from a device, the events view option shows the real-time view of events occurring at that particular device.
3. **Device Based Events View**: The Events View brings up all the real-time events occurring at the device. Each event displayed expatiates upon Source IP, Destination IP, Virtual Device, Rule, User Name, Category, Date & Time, Group Name, Device Type, BII, Flow, Protocol, Event description, Event ID, Destination Port, Attack ID, Virus Name, Interface, URL, Virus ID, and Device Name. Using the real-time Event Viewer, details on all requests that result in an emergency are readily available, such as the requests that triggered it, where it came from, what device was attacked and the port of attack.
4. You can access the other Options- Workbench, QuickVue details again from any event on the Events View.
5. Click on the icon present in the Events view window to expand the tool bar. The tool bar contains the following tools:
    - **Snap** - Use this tool to take a snapshot the current events-view (monitor)
    - **Print** - Use this tool to take a print out of the current events view
    - **Save Monitor**- Use this tool to save the current monitor for future references. The saved monitor is populated on the Manage Monitor window. See the "Events Monitors" section in Manage Monitors for more details.

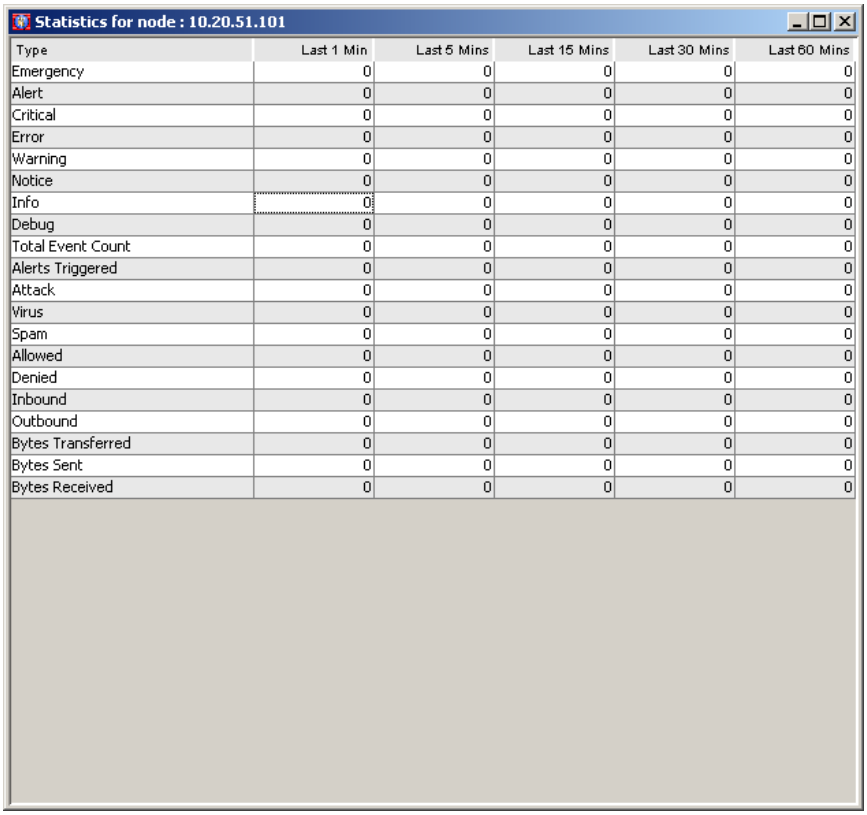


View Stats

The millions of events flowing through the devices would serve no purpose, unless they are analyzed to identify, notify and respond to suspicious behavior, malicious activity and policy violations. With numerous devices configured on NSA, it is not easy to track the latest events on any selected device. To accomplish this, NSA provides **View Stats** option in the Quick launch Options menu.

Follow the steps given below to know the Event View of the source of the event:

1. Right-Click on the node name or IP, a window pops-up with list of available Options.
2. Select the **View Stats** option from the list.
3. The Statistics window opens displaying all Types of Events and their respective count in last 1 min, 5 min, 15 min, 30 min and 60 min.
4. You can gain insight into the events status of a device or host from this option and immediately take note of any alarming event count, which can be of fatal consequences.

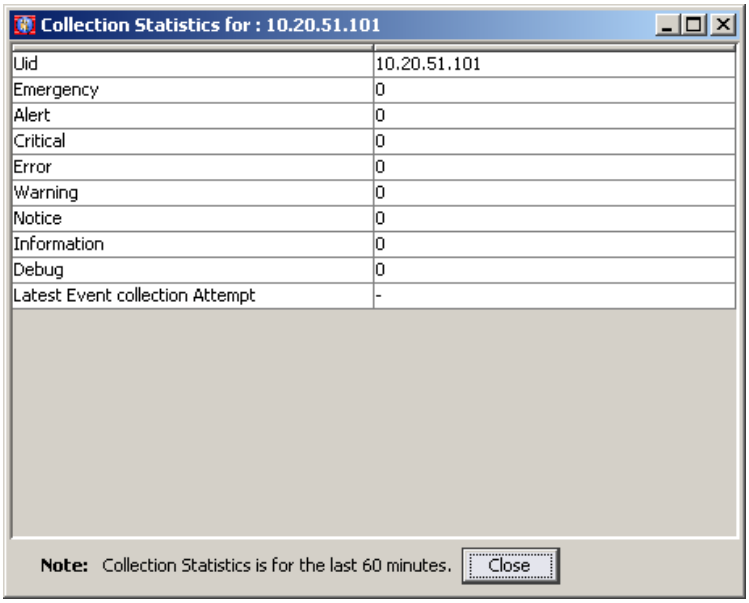


Type	Last 1 Min	Last 5 Mins	Last 15 Mins	Last 30 Mins	Last 60 Mins
Emergency	0	0	0	0	0
Alert	0	0	0	0	0
Critical	0	0	0	0	0
Error	0	0	0	0	0
Warning	0	0	0	0	0
Notice	0	0	0	0	0
Info	0	0	0	0	0
Debug	0	0	0	0	0
Total Event Count	0	0	0	0	0
Alerts Triggered	0	0	0	0	0
Attack	0	0	0	0	0
Virus	0	0	0	0	0
Spam	0	0	0	0	0
Allowed	0	0	0	0	0
Denied	0	0	0	0	0
Inbound	0	0	0	0	0
Outbound	0	0	0	0	0
Bytes Transferred	0	0	0	0	0
Bytes Sent	0	0	0	0	0
Bytes Received	0	0	0	0	0

View Collection Stats

Use this option to view the collection statistics of System, Security, Application Events, DNS Server Events, Directory Service Events and File Replication Service Events pertaining to the

selected host. Event count for severities from Emergency to Debug levels are displayed for a device.



Drill Down

NSA provides in-depth, drill-down facility to document the specific granular details of the network activity through the reports and monitors. Reports in the security center or the dashboard monitors are complemented by drill-down capabilities applicable to several event attributes such as: Destination Port, Priority, Protocol, Destination IP, Virus, Username, Event ID, Device Type, Trap count, URL, Event count and so on.

NSA provides easy menu option to drill down from the main gauges and report attributes to excavate specific granular details. This capability allows an administrator to quickly trace unusual activity to the source of the problem. You can investigate and analyze further into sources of the threats, and hence build compelling macro or micro reports.

The Reporting Drill down can facilitate two types of information:

- Breakup of the Analyzed information.
- Information related to the Analyzed Data.

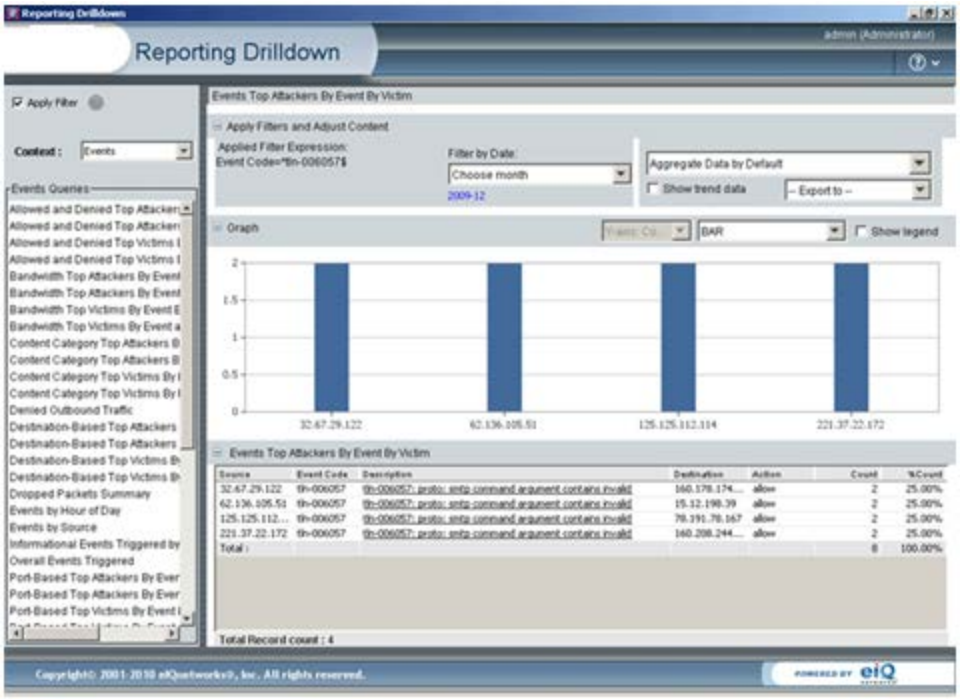
Example for Drilldown to retrieve Breakup of the Analyzed information

1. Select any node from the node summary monitor on the Dashboard window. Right-click on the node name/IP, say - Host-10.0.05.63 and select Drilldown option from the quick launch menu list.
2. The Reporting Drilldown window opens, the node filter being 10.0.05.63. Along with the device based general summary all the queries akin to Device are displayed in the TOC.

3. Let's assume that you want to get a further break-up of the Failure Events, to know as to what attributed to their occurrence. Right-Click on the Failure Events row present on the Report. The context sensitive launch options menu opens. Select Drilldown from the list.
4. The next Drilldown displays all the queries related to the Failure Events, which contain data, on 10.0.05.63. The report displays the Break-Up of the Failure Events based on event code, facility type, user name and their corresponding description and count.
5. For further break-up pick up any entry from the report and Drilldown to retrieve more concise information.

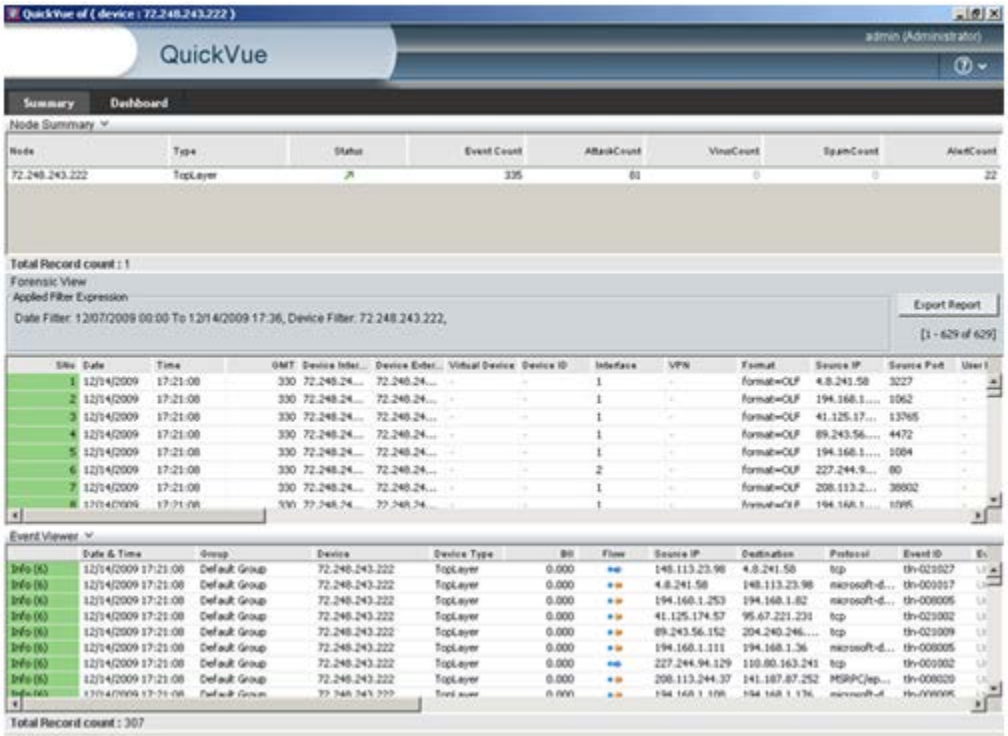
Example for Drilldown to retrieve the Related Information

1. Select any node from the node summary monitor on the Dashboard window. Right-click on the node name/IP, say - Host-10.0.05.72 and select Drilldown option from the quick launch menu list.
2. The Reporting Drilldown window opens, the node filter being 10.0.05.72. Along with the device based general summary all the queries related to device are displayed in the TOC.
3. Select a query from the TOC, let's say Top Failed Logons. The Report displays all the Failed Logon events on 10.0.05.72, including their corresponding event code, count and description.
4. Now if you want to retrieve more related information about a particular event code, let's say 529, then right-click on 529, and select Drill Down from the context sensitive launch menu.
5. The next level of Drill Down report displays all the directly and indirectly related queries on the Failed Logon events on 10.0.05.72, like queries on Account Logouts, Account Deletions and Additions, Certification Services, Failed Logon , Object Deletion and many more.
6. You can refine the Drilldown by using selecting the parameter on which you want to view the related information. Select a parameter from the Context drop-down list. In this case the contexts are Security Events, All events, Overall host events, System and Application events.
7. Select the parameter from the context drop-down list to view related information.
8. You can continue to Drill Down into the reports until you get the required details.
9. Drill Down is extremely useful when you want to generate a quick report and find out what contributed to the numbers present in the reports.



QuickVue

If you want to instantly gather all the associated details of a Device in a single view use the **QuickVue** option from the quick launch options menu. Right click on the node, and select **QuickVue** from the options list.



The QuickVue launches a portal from where you can view general and NSA specific details, of the node. You can access the following information from the main QuickVue window:

- **Summary**: The Summary tab shows the details on the selected node. The middle panel displays the Forensic data of the latest eight days on the selected node. You can also export the displayed forensic report in PDF or HTML formats and save them.
- **Dashboard**: The Dashboard displays all the panels related to the selected node that include- Panels on ports, protocols, attacks, attack sources, bandwidth, node summary, event viewer and many more.

Workbench

The Event Viewer displays all the real-time events occurring at the devices, which are configured on NSA. Right or double-click on any event from the Event Viewer. The details associated with the selected event are subsequently displayed in the Workbench dialog box.

Workbench: It is a platform where all the entities attributed to any single event compiled in the report or event viewer are displayed along with the respective 'value' details. Other than Event Viewer, users can launch workbench from different modules of the application. The workbench can be launched from the following modules:

- Monitoring
- Reporting
- Forensics
- Alerts

The following Options are available through the combo-box in the workbench to obtain further details of the selected columns (entities):

- Monitoring
- Forensic Search
- Apply Filter
- Reporting Drilldown
- Profiler Data

NOTE: -

-You can use the **Drill Down** option only on device based data.

-You can drill-down up to level 1 by using Drill Down option and **Forensic** option allows you to drill-down up to level 2.

Editing Event Attribute Values

You can edit the event attribute values from the Workbench. This saves the cumbersome task of going back to the Events and sifting through reams of data to select the desired event value. Follow the steps given below to edit attribute values and perform the required action on them.

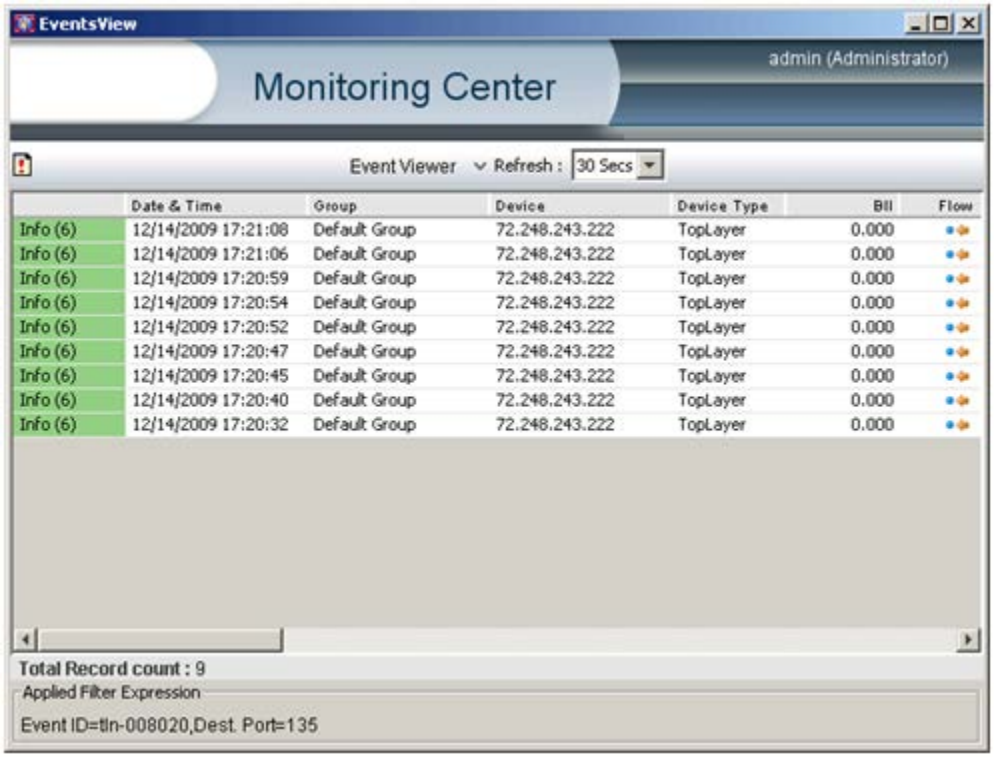
1. Double-click on the desired event to open the Workbench.
2. Select the action to be performed from the **Choose Action** combo-box.
3. Double-click on the event attribute value that you want to edit. Modify the value and press enter to save the edited value.
4. Click the **Apply** button for executing the action with the edited value.

NOTE: You can perform the Drill-down and Forensic drill down action on IP address and Port range by entering the specific range in the respective value columns.

Monitoring

Select the action type as **Monitoring** from the Workbench to view further details of the events associated with the selected column(s) (entities) bearing specific values.

1. Select Column Name(s) you want to view the details for.
2. Now click on the **Apply** button. Only those events which are associated with the chosen column(s) (entities) are displayed in a new window.



By selecting the Monitoring action from the Workbench, you can further drill information on the desired entities and obtain the events view on them. By right or double clicking any event from the Events View, you can again access the Workbench and excavate further details. You can continue excavating into events until you find the required details as you can go back to the workbench from any event on the Events View window.

Event Cache for Devices

For events generated from Cisco PIX/ASA, Cisco IOS/CatOS, FortiGate, NetScreen and Corero devices, double-clicking on Event ID attribute will result in opening an event cache URL page containing the Error Message description, Explanation and Recommended Action that should

be taken if the event messages persist from the same source. You can also access the event cache by choosing **Start > Programs > Corero Network Security Analyzer v5.1 > Event Cache Index**.

Important: In case of Cisco IOS device, to view the event details associated with the selected Event ID, manually create the eventcacheURL.ext file in the application path containing the information of CISCO Network Security Database Documentation in the following format: 29~<URL of CISCO Network Security Database Documentation>.

Forensic

Select the action type as **Forensic** from the workbench to see the Forensic report on the selected event attribute. Select any event attribute from the workbench column and then click the Apply button and specify the date and record count details on the next window.

Specify Date and Record Count Details

Applied Filter Expression: This window shows the Applied Filter Expression that was selected from the previous window (main workbench window) and applied to the Forensic drill down

Date Range: Select a Date range to consider the forensic data available in that particular time span. The following Date options are available:

- Today
- Yesterday
- All dates (Current Month dates)

Specify Date: Pick up a From and To date from the calendar icon and specify the respective time in hh:mm format from the drop-down list.

Record Count: Specify the number of Records to be displayed in the Forensic drill down report. There are two options available:

Record Count: Select the number of records from the in-built Record count list

All: Select All to display all the records available in the forensic logs that match the applied filters on the workbench to drill down.

NOTE: If you opt to include all records in the forensic drill down report the report generation process will from the tremendously slow down.

Forensic Drill-Down Report Output

A window opens displaying the forensic report based on the applied filter expression (event attribute), for example, event code, protocol, event id and so on.

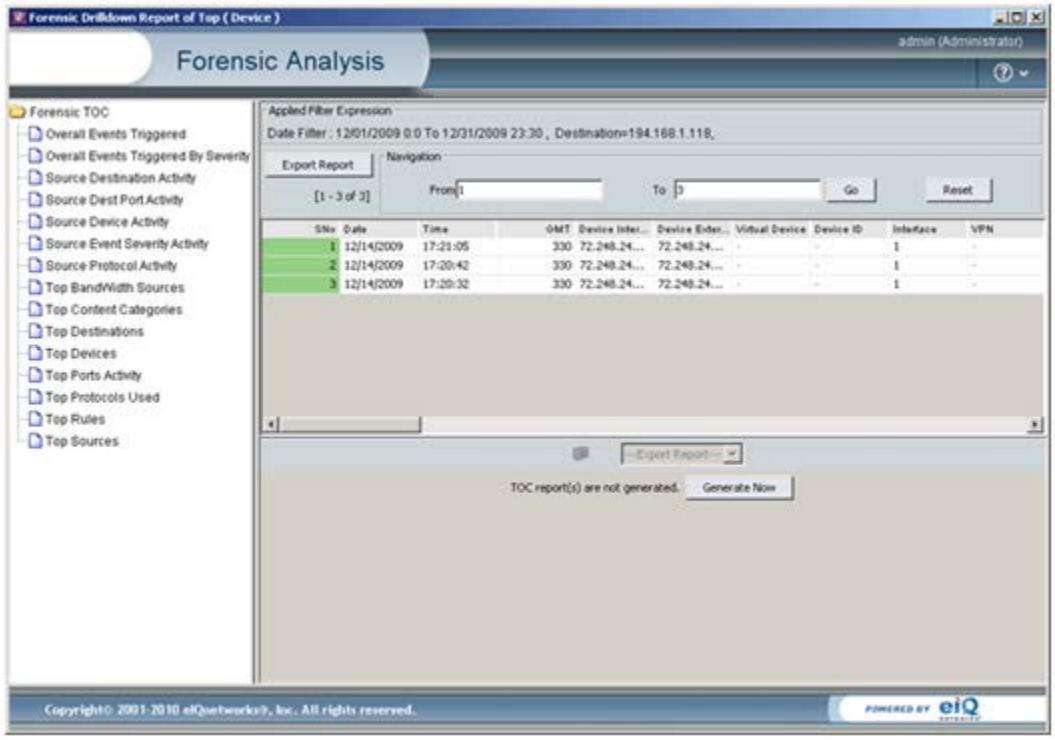
You can investigate on the event details by using the Forensic option up to two levels. The Forensic report generated from the workbench is similar to the one generated from the Forensics main module.

The Forensic report on the selected filter expression can be exported to desired location in a customized view. Use the following options to customize your report view:

- **From-To** - To specify records within a range. By default only 25 records are displayed in the forensic drill-down report. To specify a different range, you need to modify the number of records from forensicDrillCol.ext file found in the installation path.

NOTE: The specified range cannot exceed more than 1000 records.

- **Export Report** - You can export the forensic report to a specific location and in HTML or Text format. To customize the view of the exported report, select the fields you want to include in the report that is being exported.



NOTE: Values in a report saved in text format are separated by a comma separator.

Forensic drill-down from Workbench is almost similar to the main Forensic Search module, in addition to the regular features it supports the regular expressions like- '*' . For example, you

can edit the attribute value and insert a regular expression to track down the events that contain a common string in their event attribute values.

This support is available for forensic search from Workbench for following filters:

- Content Category
- Spam Source Mail
- Spam Destination Mail
- URL

Apply Filter

On the Workbench from the Reports, selecting the action type as Apply Filter provides the ability to drill-down into a report to obtain further details. This is extremely useful when you want to study the behavior of a specific user or find out what contributed to the numbers present in the reports.

You can select the event attributes from the workbench column, apply them as filters and generate a report on it. You can perform hierarchical investigation only up to one level. After accessing the workbench the second time from the consecutive report, you cannot delve and investigate any further.

Reporting Drill Down

From the Choose Action combo-box, select the Drill Down option to drill down further on the event attributes. This is extremely useful when you want to generate a quick report and find out what contributed to the numbers present in the reports.

NOTE: Since the drill-down is performed on the data present in the Forensic Summary files, it is faster than the forensic drill-down.

You can investigate on the event details by using the Drill Down option only up to first level. After you access the workbench the second time from the consecutive Drill Down report, you cannot perform investigate any further.

NOTE:

-For events occurring on devices that belong to more than one group, drill-down cannot be performed.

-Filter attributes in grey color background cannot be selected to drill-down further. For example Date & Time, Event Description and Native Log filter attributes cannot be selected in the workbench image seen on this page.

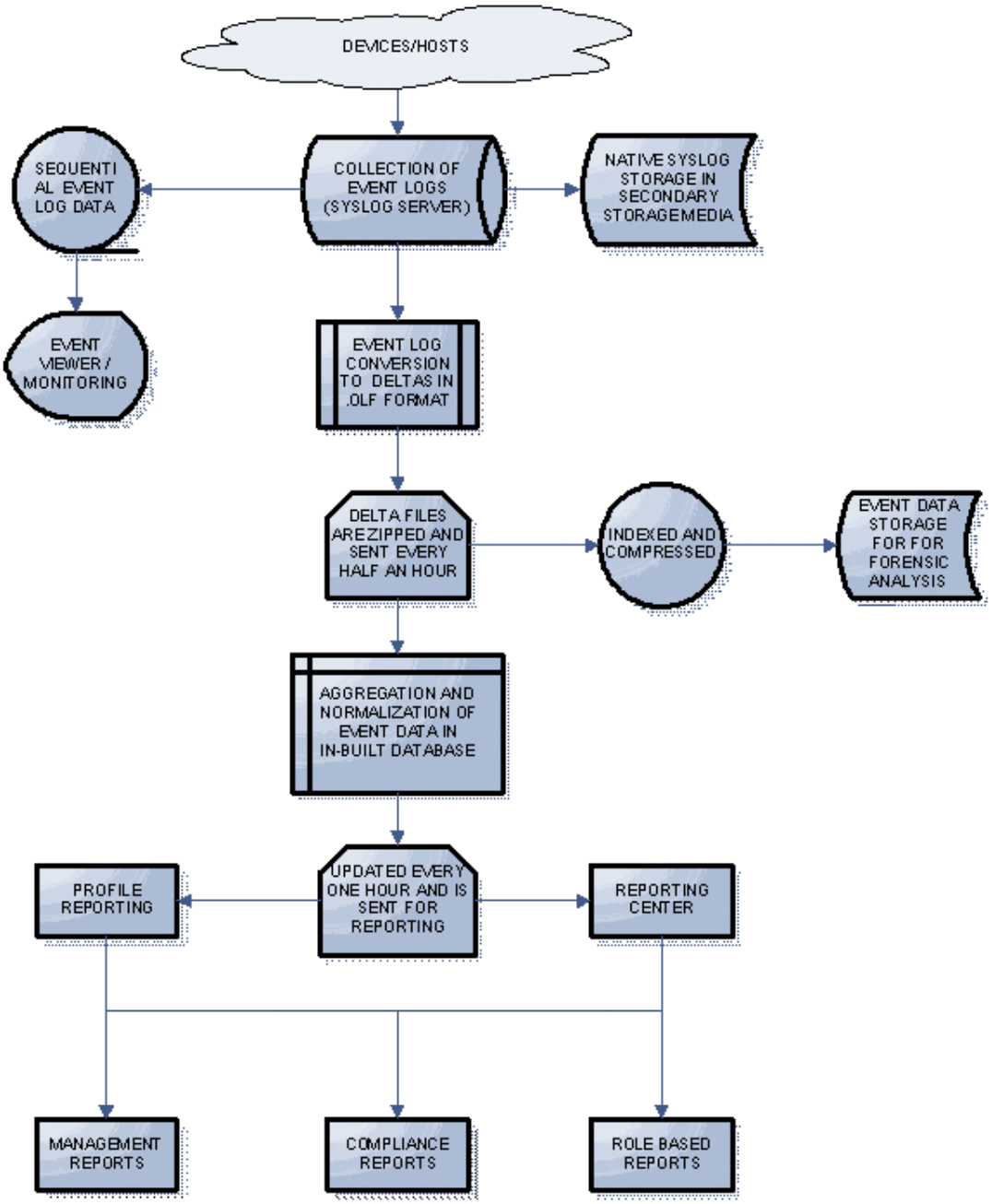
-Double-click on filter attributes shown in blue color to see the description in a dialog box.

-To negate the filter in the reports, select the Negate Filter check box on the workbench.

Chapter 24: Flow Charts

Click on the below link to view the complete process (Flow Chart) of **Security Information** and **Event Management**.

SIEM FLOW CHART



Chapter 25: Appendix

Backing up NSA 5.1

Although NSA 5.1 has file replication (auto backup) when running in a distributed mode it is still a good idea to backup your data.

Backing Up Data from an NSA 5.1 Server

To backup data from a NSA server, follow the instructions below.

1. Logon to your NSA Server. If you have a distributed environment you will need to follow step 2 for all regional and central servers.
2. The default install path for NSA is Root://CoreroNSACentral. If you did not install NSA in the default path then you will need to change the path to the appropriate location. You will need to backup the following files and directories from the NSA directory:
    - Database
    - ForensicLogs
    - Profiles
    - Userprofiles
    - Devices.xml (Only if you have devices)
    - Groups.xml

Backing Up Data from an NSA 5.1 Data Collector

1. The NSA Data Collector may be installed on the same physical server as the NSA Server or it may be installed on a separate server. Please be sure to backup all instances of the NSA Data Collector within your environment.
2. The default install path for the NSA Data Collector is Root://NSADataCollector. If you did not install the NSA Data Collector in the default path then you will need to change the path to the appropriate location. You will need to backup the following files and directories from the Syslog directory.
    - Logs
    - DeviceLicInfo.txt
    - FirewallList.txt (Only if you have network devices)
    - Leafirewalls.txt (Only if you have Check Point Firewalls)
    - RDEPDevices.txt (Only if you have RDEP Devices)

Appendix A: Regular Expressions

NSA supports the standard operators '\', '.', '?', '*', '+', '[]', '()', '|', '^', and '$' to define the Regular Expressions.

- '\' escapes the character that follows it, so that it will not behave specially. If you want to match one of the special characters listed above, you need to precede it with a '\' so it won't be interpreted as an operator. This includes '\' itself. If you want to search for "C:\Program Files\", you need to use the regular expression "C:\\Program Files\\".
- '.' matches any one character. Be careful: it does not only match the '.' character! The regular expression "1.3" matches "123". If you want to match only '.', you must escape it with '\': "\.\.\." matches only the string "...".
- '?', '*', and '+' match varying numbers of whatever precedes them. '?' matches zero or one occurrence - it means "optional". '*' matches zero or more - it means "any number". '+' matches one or more. Be careful: '*' does not mean "match any string" as it does in Unix filename globbing! To match any string, use ".*" - "any number of any character".
- '[]' enclose sets of characters, and match any one of those characters. Ranges of characters can be written with a hyphen: "[a-b]" matches anything between 'a' and 'b'. For example, "[0-9]" matches any digit; "[a-zA-Z]+" matches any word of alphabetic characters.
- '()' group items so '?', '*', and '+' can operate on them. For example, if you want to match a sequence of comma-separated integers, you could use "([0-9]+,)*[0-9]*". The parentheses allow the first '*' to repeat a sequence of integers and commas.
- '|' separates alternatives (usually in parentheses). For example, "(+|-|)" matches either "+", "-", or nothing - it's equivalent to "[+\-]?".
- '^' and '$' prevent a regular expression from matching anywhere within a string. Normally regular expressions match any part of a line - they act as if they had ".*" appended to the beginning and the end. If the regular expression begins with '^', then it only matches at the beginning of a string or line. If it ends with '$', it only matches at the end. These characters are not special in any other position - "a$b" still matches only the string "a$b". For example: If you were searching an XML file for start and end tags of section elements, you could use "</?section([^>]*)?>". Both the '/' and any arguments are optional. "</?section[^>]*>" wouldn't work, because it matches other elements, e.g. "<sectionSummary>".
- "-?[0-9]*\.[0-9]*" matches any signed decimal number.