User Guide

ManageEngine

OpManager

www.opmanager.com

Table Of Contents

ManageEngine OpManager - Network Monitoring Software

With the growing need for the network monitoring software in the IT industry, OpManager has been built to satisfy the needs of network administrators by monitoring servers, routers, switches, firewalls, printers, critical services and applications from a single console.

Network Monitoring Software

ManageEngine OpManager is a comprehensive network monitoring software that provides the network administrators with an integrated console for managing routers, firewalls, servers, switches, and printers. OpManager offers extensive fault management and performance management functionality. It provides handy but poweful Customizable Dashborads and CCTV views that display the immediate status of your decives, at-a-glance reports, business views etc. OpManager also provides a lot of out-of-the-box graphs and reports, which give a wealth of information to the network administrators about the health of their networks, servers and applications.

OpManager's network monitoring functionality includes the following:

Network Monitoring: OpManager discovers switches, routers and firewalls in the network during the network discovery automatically and monitors the critical parameters such as the traffic rate, error and discards rate, buffer hits and misses and so on. You can get the availability report of each port and interface. Using the Switch Port Mapper tool, you can get the list of devices connected to each port of the switch. You can also create your own views and draw the diagram to virtually represent your network and get the availability of the interfaces visually.

Server Monitoring: OpManager allows you to classify devices as servers and desktops. This facilitates separating critical servers from end-user workstations and allows for more meaningful management. You can manage Windows Event Logs and Windows Services.

Cisco IPSLA Monitoring: OpManager allows you to monitor the performance of your VoIP networks with the Cisco IPSLA monitor. The Cisco IPSLA monitor is add-on feature and monitors the various parameter like Latency, Jitter, MoS etc.

WAN Monitoring: OpManager provides complete solutions for monitoring your WAN links. It checks for RTT, Latency and availabilty between the WAN links. The WAN monitor comes as an add-on feature.

Applications and Services Monitoring: OpManager discovers and actively monitors services and applications running in the servers. Out-of-the-box support is provided for services such as Web, HTTPS, FTP, IMAP, LDAP, Telnet, MySQL, MS-Exchange, SMTP, POP3, WebLogic, etc., and applications such as MSSQL, MS Exchange, Oracle and Lotus. Special add-ons are available for monitoring Exchange 2000/2003/2007 and Active Directory Services.

URL Monitoring: OpManager monitors your Web sites, both global URLs and URLs in the servers, and promptly notifies you when the host becomes unavailable.

Fault Management: OpManager provides extensive solutions for monitoring Sylsogs, Eventlogs and current Processes running on the devices. OpManager detects faults in the network through periodical status polling and generates color-coded alarms for the faults. OpManager can also be configured to notify the administrator about the fault detected in the network.

Performance Management: OpManager measures the performance of the network hardware and software, such as the bandwidth, memory, disk and CPU utilization, and service response time by collecting data at regular intervals. These data are provided in the form of reports and graphs to the administrators. The threshold limits can be configured to pro-actively monitor the critical parameters in the managed devices.

Getting Started

Starting OpManager

After installation, all the OpManager-related files will be available under the directory that you choose to install OpManager. This is referred to as *OpManager Home* directory.

- Starting OpManager on Windows
- Starting OpManager on Linux
- Connecting the Web Client

On Windows Machines

If you have chosen to install OpManager as Windows service, you will be prompted to start the service after successful installation. The Web Client is invoked automatically on installing as a Service. Enter the log-on details. The default user name and password is 'admin' and 'admin' respectively.

To later start OpManager as a Windows Service, follow the steps below:

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Under **Administrative Tools**, select **Services**.
3. In the details pane, right-click **ManageEngine OpManager** and click **Start**.

To stop the ManageEngine OpManager service, right-click the **ManageEngine OpManager** service in the Services window and click **Stop**.

On Windows machines, an icon is displayed on the system tray to manage the application. You can start the client, start the server, and shut down the server using this icon.

On Linux Machines

1. Log in as '**root**' user.
2. Execute the **StartOpManagerServer.sh** file present in the <*OpManager Home*>*/bin* directory.
3. Once the server is started successfully, execute **StartOpManagerClient.sh** to start the client. In the displayed login window, type the **User Name** and **Password** and press Enter.

To stop OpManager running on a linux machine, execute the **ShutDownOpManager.sh** file present in the <*OpManager Home*>*/bin* directory.
Type the **User Name** and **Password** in the Shut Down OpManager window and press Enter.

Connecting the Web Client

1. Open a JavaScript-enabled Web browser such as Internet Explorer or Mozilla Firefox.
2. Type http://<**host_name**>:<**port_number**> in the address bar and press Enter. Here, <**host_name**> is the name of the machine in which OpManager is running and <**port_number**> is the port that you have chosen to run OpManager Web Server during installation.

   [Note: If you have enabled SSL, connect as https:///<**host_name**>:<**port_number**> in the address bar and press Enter.]

3. Type the **User Name** and **Password** and click **Login**. The default user name and password are 'admin' and 'admin' respectively.

Alternatively, if the OpManager server is running on Windows machines, you can start the Web client using Start > Programs > ManageEngine OpManager > OpManager Web Client.

[OR]

Right-click the tray icon and select **Start Client** option.

From OpManager build 7010 onwards we provide SSL support for the webclient. Click here to enable SSL.

Enabling SSL in OpManager

OpManager (build 7010 onwards) supports SSL.

Here are the steps to enable SSL:

1. Stop OpManager Service.
2. Open a command prompt and change directory to /opmanager/bin.
3. Execute the script OpManagerService.bat with **-r** option as shown below:

   OpManagerService.bat -r

   This removes the Service entry.

4. Rename the folder called **apache** under /opmanager to **apache-old**.
5. Click here to download the SSL-enabled Apache.
6. Extract the zip file on /opmanager folder such that a new **apache** folder is seen under /opmanager.
7. From the command prompt, with /opmanager/bin as the current directory, execute the script **ssl_gen.bat**. This creates the SSL Certificate.
8. Now, execute the OpManagerService.bat script once again, but with the argument as **-i** as shown below. This recreates the OpManager Service.

   OpManagerService.bat -i

9. Restart OpManager Service and connect as https://<opmanager host name or IP address>:<port number>. For instance, if the host name is OpM-Server and the port is 80, you will connect as

   https://OpM-Server:80

The WebClient is now SSL-enabled.

Registering OpManager

You can register OpManager by applying the license file that you receive from AdventNet. To apply the license, follow the steps given below:

1. Click **Register** at the top right corner of the client page.
2. Click **Browse** and choose the license file from the location it is saved.
3. Click the **Register** button to apply the license file and close.

Should you encounter any errors when applying the license, contact Support with the license error code.

Configuring Failover Support for OpManager

Failover or redundancy support for OpManager is necessary to achieve uninterrupted service. It becomes cumbersome if the OpManger DB crashes or loses its network connectivity and not monitoring your network. Though regular backups help you recover from DB crashes, but it takes time for OpManger to resume its service. However, in the mean time your network will be left unmonitored and some other critical devices such as routers, mail servers etc. may go down and affect your business. Implementing a redundancy system helps you to overcome such failures.

Failover support requires you to configure OpManager Secondary or Standby server and keep monitoring the OpManager Primary server. Incase the Primary server fails the Standby server automatically starts monitoring the network. The transition is so quick and smooth that the end user does not feel the impact of the failure of the Primary server or the subsequent taking over by Standby. In parallely the Standby server triggers an email alert (email ID entered configured in the mail server settings) about the Primary's failure. Once the Primary server is restored back to operation the Standby server automatically goes back to standby mode.

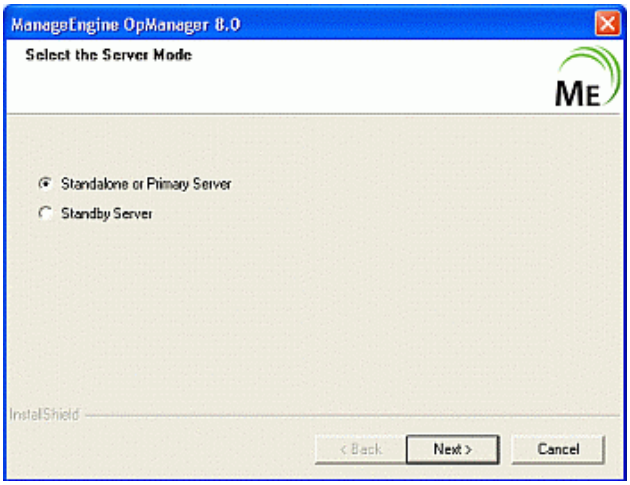
Working Mechanism

The Primary server updates its presence with a symbolic count in the BEFailover table at a specified interval known as the HEART_BEAT_INTERVAL. With every update the count gets incremented. This count is known as LASTCOUNT. Similarly the standby server also updates the its presence by updating the LASTCOUNT in the BEFailover table.

When the Primary server fails, it fails to update the LASTCOUNT. The Standby server keeps monitoring the Primary's LASTCOUNT at a specified periodic interval known as FAIL_OVER_INTERVAL. By default the FAIL_OVER_INTERVAL value is 60 seconds. If required you can modify it in the Failover.xml file (<OpManager_Standby_home>\conf). Supposing, you have specified FAIL_OVER_INTERVAL as 50 seconds, the standby will monitor the Primary's LASTCOUNT for every 50 seconds. Every time, when the Standby server looks up the LASTCOUNT, it compares the previous and present counts. When the Primary server fails to update the LASTCOUNT, consecutive counts will be the same and the Standby assumes that the Primary server has failed and starts monitoring the network.

Installing the Primary Server

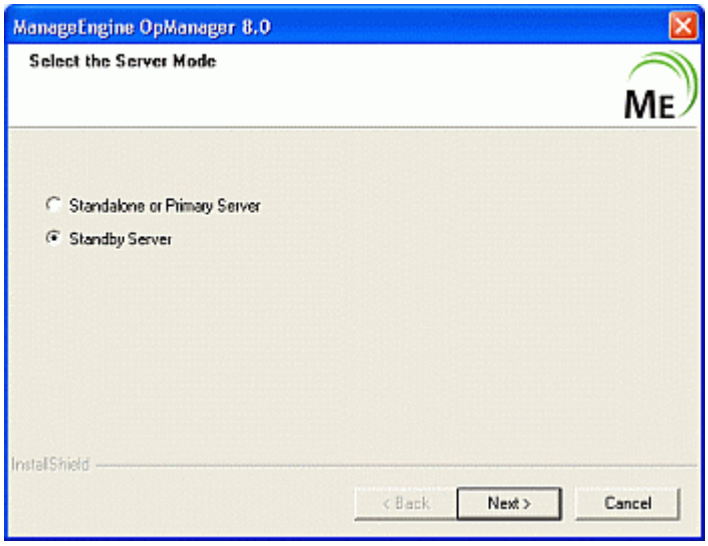
If you are already running OpManager, first upgrade to build 7260 before applying build 8000. If you installing OpManager for the first time directly install build 8000. While installing OpManger (build 8000) on the Primary server, select as Primary server in the installation wizard and complete the installation process. Start the Primary server.



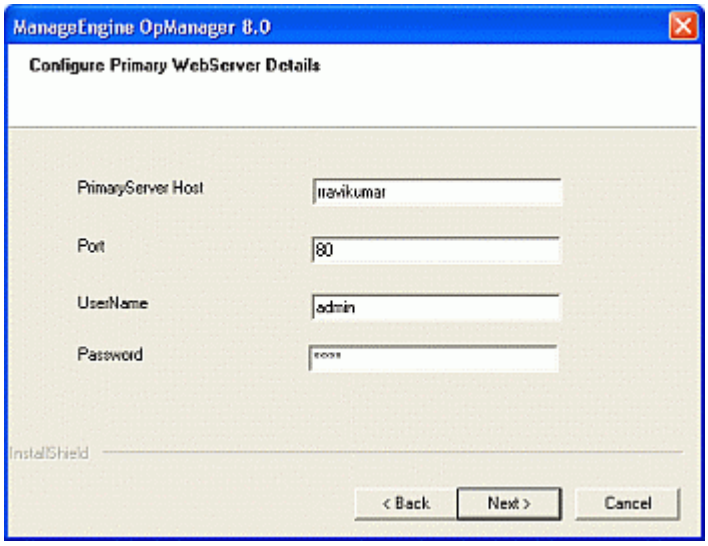
Installing the Standby Server

While installing OpManager on the standby server,

1. Select as Standby server mode in the installation wizard.



2. Enter the Primary webserver host, port and login details and complete the installation. Do not start the Standby server.



Note: The Date and Time settings of the Primary and the Standby should be same.

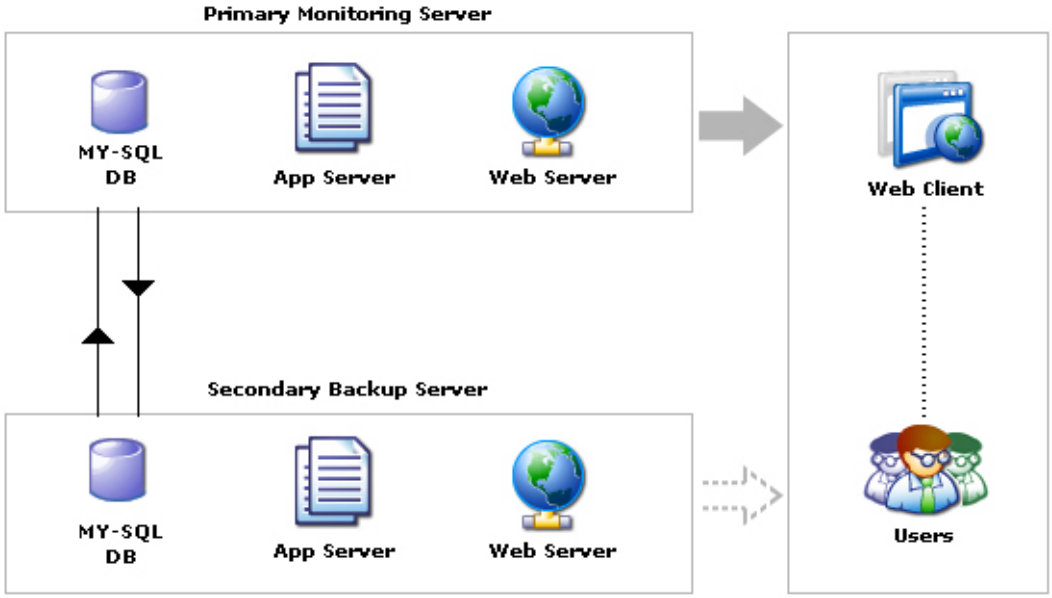
Configuring Failover:

The procedures for configuring failover support varies according to the following cases (backend DB used):

- Using MySQL bundbled with OpManager
- Using Standalone MySQL server
- Using MSSQL

Using MySQL as the backend DB

Using MySQL bundled with OpManager:



If you are using MySQL bundled with OpManager as the backend DB, then follow the steps given below to copy the contents from the primary DB to the standby DB.

1. Stop the OpManager Primary server.
2. Open the command prompt in the Primary server and execute the command startMysql.bat/startMysql.sh (<OpManager_Primary_home>\bin).
3. In the Standby server, open the command prompt and execute the command ReplicateDB.bat/ReplicateDB.sh (<OpManager_Standby_home>\bin)
4. After successfully replicating the DB from Primary to Standby server, execute the command stopMysql.ba/stopMysql.sh (<OpManager_Primary_home>\bin) in the Primary server.
5. Start the OpManager Primary server.
6. Start the OpManager Standby server.

Using Standalone MySQL:

Steps to be followed on the Primary server:

1. Stop the Primary server.
2. Apply build 7260 before applying build 8000.
3. Upgrade the Primary's remote MySQL (standalone MySQL server) to version 5.0.46.
4. Copy my.huge.ini/mu.huge.inf files from the Primary server and paste it under the Primary's remote MySQL installation directory.
5. Copy the Primary OpManager DB and its details to the Primary's remote MySQL server by
    1. Copying the OpManager DB folder and ibdata and ib_logs files (available under <OpManager_Primary_home>\mysql\data) and pasting it under the Primary's remote MySQL installation directory.

       or use mysql dump utility:

       Configurations to be done in the Primary server:

    2. Run startMySQL.bat or startMySQL.sh (<OpManager_Primary_home>\bin) inorder to start the MySQL server.

3. Connect the MySQL bundled with OpManger using MySQL client and assign privileges to access this DB from the remote MySQL by entering the following command:
   grant all privileges on *.* TO root@ '<Primary's_remote_mysql_machine_name>'
4. Now go to the remote MySQL server and verify whether it is able to connect to the Primary server by entering the following command:
   mysql -u root -P 13306 -h <Primary_server_name>

   Configurations to be done in the Primary's remote MySQL server:
5. Start the remote MySQL application 5.0.46 if not started after the upgrade.
6. From the command prompt itself go to the bin directory of the MySQL installation.
7. Connect to the MySQL client and create a database OpManagerDB. The name of the database should be the same of the Primary's.
8. Backup the MySQL data in the Primary server using the following command:
   mysqldump -u root -P 13306 -h <Primary_server_name> OpManagerDB > opm.sql
9. Restore the data into the new installation using the following command:
   mysql -u root -P mysqlport OpManagerDB < opm.sql

6. Ensure that OpManager Primary server has started successfully.
7. Stop the OpManager Primary server.
8. Now apply the build 8000.
9. After successfully upgrading to build 8000, add the following script in mysql server startup script in Primary's remote MySQL server.
   For Windows installations: **--default-files = <mysql_installation_path>\my.huge.ini**
   For Linux installations: **--default-files = <mysql_installation_path>\my.huge.cnf**

Steps to be followed on the Standby server:

1. Directly install 8000 build.
2. Install MySQL version 5.0.46 or above on the Standby's remote MySQL DB machine and start the MySQL.
3. Copy my.huge.ini/my.huge.cnf files from the standby server and paste it under the standby's remote MySQL installation directory.
4. Copy the Standby OpManager DB and its details to the Standby's remote MySQL installation directory by
   1. Copying the OpManager DB folder and ibdata and ib_logs files (available under <OpManager_Standby_home>\mysql\data) and pasting it under the Standby's remote MySQL installation directory.

      or use mysql dump utility:

      Configurations to be done in the Standby server:

   2. Run startMySQL.bat ot startMySQL.sh (<OpManager_Standby_home>\bin) inorder to start the MySQL server.
   3. Connect the server using MySQL client and assign privileges to access this DB by the remote MySQL DB by entering the following command:
      grant all privileges on *.* TO root@ '<Standby's_remote_mysql_machine_name>'
   4. Now go to the Standby's remote MySQL server and verify whether it is able to connect to the Standby server by entering the following command:
      mysql -u root -P 13306 -h <Standby_server_name>

      Configurations to be done in the Standby's remote mysql server:
   5. From the command prompt itself go to the bin directory of the MySQL installation.
   6. Connect to the MySQL client and create a database OpManagerDB. The name of the database should be the same of the Standby's.

7. Backup the MySQL data in the Standby server using the following command: **mysqldump -u root -P 13306 -h <Standby_server_name> OpManagerDB > opm.sql**
8. Restore the data into the new installation using the following command: **mysql -u root -P mysqlport OpManagerDB < opm.sql**

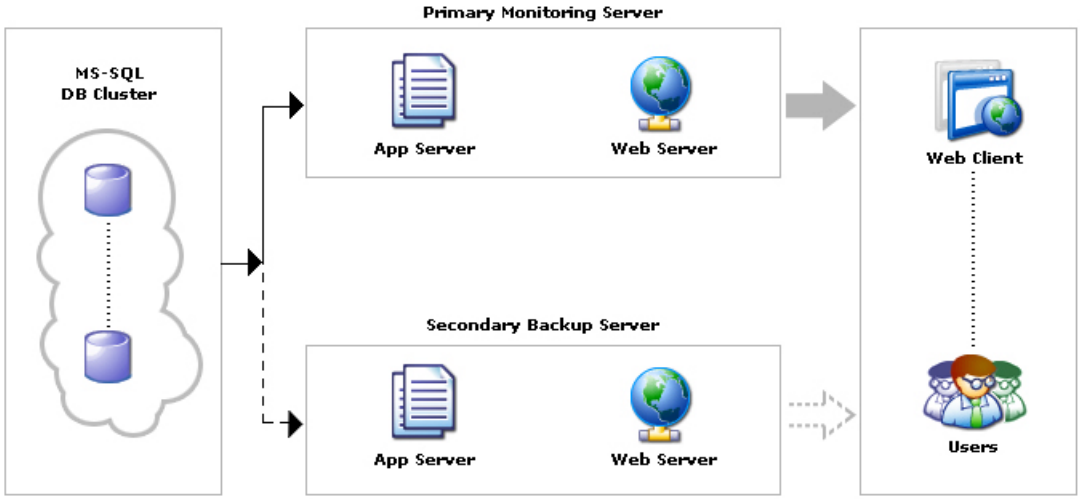
5. After successfully restoring the Standby OpManager DB to its remote MySQL server, add the following parameter in mysql server startup script in the Standby's remote MySQL server.
   For Windows installations: **--default-files = <mysql_installation_path>\my.huge.ini**
   For Linux installations: **--default-files = <mysql_installation_path>\my.huge.cnf**

Now start the Primary and Standby OpManager servers and their respective remote MySQL servers.

Using MSSQL as the backend DB

If you are running OpManager with MSSQL as the backend DB, then implement clustering. Clustering refers to an array of databases in which the data are stored and have a single virtual IP. If any of the DB in the cluster environment fails the other DBs have the data thereby providing high availability of data. The Primary server sends all its data to a virtual IP and the data gets stored in multiple locations. The Standby server that takes control over the network in case the primary fails, then the standby server also sends the data to the same virtual IP.

For configuring MSSQL server clustering visit the below link published by Microsoft.
http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/failclus.mspx#EDAAC



For MSSQL, the Standby OpManager server can be started once the installation is completed, provided you have already configured MSSQL clustering for Primary server.

Once the Primary server fails, the Standby server assumes itself as the Primary server and starts monitoring the network. Once the Primary server is up, the Standby server goes back to its standby mode and monitors the Primary server.

Migrating Database

OpManager supports MySQL and MSSQL as the backend database. At a later time, you can choose to migrate from one database to another. Here are the steps:

Migrating from MySQL to MSSQL

Prerequisites

- The Build Number of OpManager must be 6000 or higher.
- MSSQL database must be installed as this is not bundled with OpManager.

Steps to migrate are,

1. Stop OpManager again and take a backup of the data using BackupDB.bat present under /bin/backup directory .
2. Select Start --> Programs --> ManageEngine OpManager --> DB Manager --> DB Configuration.
3. A DB Configuration window pops up. Select MSSQL option.
4. Configure the following information:
    1. DB Host : The name or the IP address of the machine where MSSQL is installed.
    2. Port: The port number in which OpManager must connect with the database. Default is 1433.
    3. User Name and Password: The user name and password with which OpManager needs to connect to the database.
    4. Driver Jars: Specify the path of the Database driver
    5. Click OK.
5. Restore the data using RestoreDB.bat present in /bin/backup directory and restart OpManager.

Refer to our online knowledgebase article to configure Microsoft MSSQL JDBC driver.

Data Backup and Restoration

Backup

To take a backup of the data and configurations in OpManager,

- Go to <*OpManager Home*>*/bin/backup* directory
- Execute **BackupDB.bat/sh** to start the data backup

Once the backup is over, a directory **backup** is created in <*OpManager Home*>, and the backup file with **.data** extension is placed in this directory. The name of the backup file contains the date and time at which backup is taken. Example: BackUp_FEB28_2005_15_51.data

Restoration

To restore the backed up data,

- Go to <*OpManager Home*>*/bin/backup* directory
- Execute **RestoreDB.bat/sh** with the backup file name as argument. See example below:

  C:\<OpManager Home>\bin\backup>RestoreDB.bat BackUp_FEB28_2005_15_51.data

During restoration, the existing tables are dropped, new tables are created, and the data is restored in all the tables.

Changing Ports in OpManager

You will be prompted to change Web Server port during installation. You can change it after installation.

The script for changing the Web Server port number, **ChangeWebServerPort** (in Windows this will be a *.bat* file and in Linux, *.sh* file) is available under the <*OpManager Home*>*/bin* directory.

The steps to change the port number are as follows:

1. Stop the OpManager server. If you are running OpManager as Windows service, stop the service.
2. Execute the script as follows:
   In Windows,
   ChangeWebServerPort <old_port_number> <new_port_number>

   In Linux,
   sh ChangeWebServerPort.sh <old_port_number> <new_port_number>

   Here, old_port_number is the port number you specified during installation and new_port_number is the one where you want to run the Web server.
3. Start the OpManager server.

Changing Other Ports

You can also change the port by editing the value of WEBSERVER_PORT=80 in the file /conf/Port.properties.

You can change the following ports too in this file if the default ports are occupied:

WEBCONTAINER_PORT=8009
NMS_BE_PORT=2000
WEBSERVER_PORT=80
TOMCAT_SHUTDOWNPORT=8005
RMI_PORT=1099

Quick Start with Intro tab

The Intro tab provides you the settings that have to be configured one after the other (starting from configuring credentials, discovering devices to scheduling reports) for quick and complete deployment of OpManager. Further it provides you the video demos and the step by step procedures required for configuring each and every setting.

The Intro tab also facilitates you to register for free technical support during the trial period. Click on Register Now button to register for free technical support.

Note: Intro tab is displayed only for users with Full access previleges to all devices.

What Should Be Monitored?

Active network monitoring is a must to gain accurate and real-time visibility of the health of your network. However frequent monitoring can become a huge strain on your network resources as it generates a lot of traffic on the network, especially in large networks.

We recommend monitoring only the critical devices on the network. This is a best practice adopted by the network administrators worldwide.

Following are the components of networks that are considered critical:

- WAN Infrastructure: Routers, WAN Switches, Firewall, etc.
- LAN Infrastructure: Switches, Hubs, and Printers.
- Servers, Services, and Applications: Application Servers, Database servers, Active Directory, Exchange Servers, Web servers, Mail servers, CRM Applications, etc.
- Host Resources: CPU, Memory, and Disk Utilization of critical devices.
- Critical Desktops and Workstations.

Monitoring Interval for a Device Category

OpManager allows you to set a common monitoring settings for all the devices under a specific category.

To do so, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Monitoring**, click **Monitoring Intervals**.
3. To enable monitoring for a category, select the check box under **Enable** corresponding to the category and type the monitoring interval in minutes, in the adjacent box.
   To disable monitoring a specific category, clear the respective check box.
4. Click **Save** to save the settings.

For instance, if you want to monitor servers every minute, ensure that the check box corresponding to **Servers** is selected and type 1 in the adjacent box.

How Frequently Should I Monitor?

The general practice is to monitor critical devices more frequently than non-critical devices.

Given below are the recommended monitoring intervals for small and medium-sized networks (up to 1000 devices):

- Routers and Critical Servers: 10 minutes
- Switches, Hubs, and Printers: 10 - 20 minutes
- Critical Services like Exchange, Active Directory: 10 - 20 minutes
- Desktops and Workstations: We recommend turning off monitoring for desktops and workstations to reduce the amount of network traffic generated by OpManager.
  This is done by removing selection for Desktop category in Admin > Monitoring Intervals.
  Alternatively, monitor them less frequently, say for every hour or 30 minutes.

  If there are a few critical workstations that you want to monitor, you can turn on monitoring for those devices individually.

Personalize WebClient

Change Password

You can change the WebClient login password. Click on the **Personalize** link in the WebClient and select the **Change Password** tab. Provide the current password and the new password. Retype new password to confirm. The next time you login, use the new password.

Select Skin

From the Personalize link, select the **Skin Selector** tab to select the required skin for the WebClient.

Configure Automatic Refresh

From the Personalize link, select the **Automatic Refresh** tab to set automatic page refresh at the selected interval. You can also set the session timeout interval here.

Discovery

Add Credentials

OpManager accesses the remote devices using the protocols SNMP, CLI, or WMI. The credentials like the password/snmp community, port etc., may differ for different device types. Pre-configuring a set of credentials in OpManager helps applying them to multiple devices at a time, saving a lot of manual effort.

1.Go to Admin --> Credential Settings
2.Click New in this screen
3.Configure the following parameters and click Add to add the credentials:

Credential Type: Select the relevant protocol.

SNMP v1/SNMPv2: SNMPv1 and SNMPv2 are community based security models. Enter the Credential name and description. Configure the correct Read and Write community, and the SNMP Port.

SNMP v3: SNMPv3 is a user based security model. It provides secure access to the devices by a combination authenticating and encrypting packets over the network. The security features provided in SNMPv3 are Message integrity, Authentication and Encryption. If you select SNMPv3 as the credential type, then configure the following parameters.

1. **Name**: Enter the name of the credential.
2. **Description**: Enter a brief description about the credential.
3. **User Name**: Enter the name of the user (principal) on behalf of whom the message is being exchanged.
4. **Context Name**: An SNMP context name or "context" in short, is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context. An SNMP entity potentially has access to many contexts. In other words, if a management information has been defined under certain context by an SNMPv3 entity, then any management application can access that information by giving that context name. The "context name" is an octet string, which has at least one management information.
5. **SNMP Port**: Enter the SNMP port number.
6. **Authentication**: Select any of the authentication protocols either MD5 or SHA and enter the password. MD5 and SHA are processes which are used for generating authentication/privacy keys in SNMPv3 applications.
7. **Encryption**: Select any of the encryption protocols either DES or EAS-128 and enter the password. Note: Only after configuring Authentication it is possible to configure Encryption.

WMI: If you select WMI as the protocol, configure the Domain Name, the user name, and the password. Example:- *TestDomain\TestUser.* Also enter the credential name and description.
Telnet/SSH: Enter the credential name and description. For Telnet/SSH, make sure you configure the correct login prompt, command prompt, and password prompt besides the user name and password to access the device.

The SNMP credentials created is used during the initial discovery and classifications. OpManager uses these credentials to classify and add the devices into OpManager.

Using Quick Configuration Wizard

You can also use the Quick Configuration Wizard to associate a service to several devices at one go. Here are the steps:

1. From the Admin tab, select Quick Configuration Wizard.
2. Select the option **Associate a credential to several devices** and click Next.
3. All the available Credentials are listed. Select the Credential which you want to associate to your devices.
4. Select the devices to which you want to assign the credential from the column on the left and move them to the right.
5. Click Finish. The Credential is associated to the selected devices.

Discovering Networks Using OpManager

You can discover devices on a network by either specifying a range or the entire network OpManager uses ICMP/Nmap to discover the devices on a network.

Discover a range

To discover devices from a selected range specify the start and end ip address and select the netmask for the devices to be discovered within that range.

1. Click the Admin tab.
2. Under Discovery, select Discover Devices.
3. Use IP Range: Select this option to specify the range.
4. Start IP: Specify the IP address of the device in the range from where OpManager should start discovery.
5. End IP: Specify the IP address till which OpManager should discover.
6. Netmask: Select the correct netmask.
7. Discovery Credentials: Select the configured Credentials to be used for discovery.
8. Advanced SNMP Settings: Click here to configure an increase SNMP timeout or SNMP retries.

Discover a complete network

1. Use CIDR: Select this option to discover an entire network.
2. Network IP: Specify the Network IP to be discovered.
3. Credentials: Select the credentials and SNMP settings as mentioned above.
4. Click Discovery for the discovery to start.

Discover by Importing from a file

You can import a set of IP addresses for discovery from a csv file.

1. Create a csv file with the details of name/ipaddress of the device, displayname etc.
2. Browse and select the CSV file from which you want the devices discovered and imported.
3. Click here to view the CSV file.
4. Provide the correct netmask.

Import the Devices into OpManager

All the discovered devices are listed category-wise.

1. Click Import Devices to add all the devices for monitoring.
2. Click Finish once the devices are added.

Discover Individual Devices

You might have added more devices to your network and may therefore need to forcefully discover these devices. You can discover such devices on demand by following the steps below:

1. Click the Admin tab.
2. Under Discovery, select Add Device .
3. Type either the IP Address or the Device Name of the device to be discovered.
4. Select the discovery credentials.
5. Click Add Device to start discover

The device is discovered and classified properly.

Alternatively, you can also add devices to a specific category directly.

1. Go to the required map view, say Servers Map or Routers map.
2. Click the Add Server/Router/... etc option on top of the map to discover and classify the device into that particular category.

Note: If you are unable to add the device or if does not show up in the map in which you are looking for, try pinging the device from the OpManager machine and check for response. Search the device using the Device Search box on the top right corner in the WebClient.

Managing Devices

Managing and Unmanaging a Device

By default, OpManager manages all the discovered devices. However, there might be some known devices that are under maintenance and hence cannot respond to status polls sent by OpManager. These devices can be set to unmanaged status to avoid unnecessary polling. Once maintenance gets over, they can be set to managed status.

To unmanage a device

1. Go to the device snapshot page.
2. Under **Actions**, select **Unmanage**.

This stops the status polling and data collection for the device and changes the device status icon to gray .

To start managing an unmanaged device

1. Go to the device snapshot page.
2. Under **Actions**, select **Manage**.

This resumes the status polling and data collection for the device. The status icon shows the current status of the device.

To manage or unmanage many devices at a time, you can use Quick Configuration wizard of OpManager. To do so, follow the steps below:

1. In the **Admin** tab, under **Tools**, click Quick Configuration Wizard.
2. Select **Manage/Unmanage devices** and click **Next**.
3. Select the category from which you want to unmanage.
4. To stop managing the devices, move them to the list in the right. To start managing the unmanaged devices, move them to the list in the left.
5. Click **Finish**.

You can also schedule downtimes for the devices incase you do not want it monitored for a specified interval

Device Snapshot

OpManager's Device Snapshot shows the device health and that of its resources at a glance.

To view the snapshot page of the device, click the device name link in the map, or type the name of the device in the **Device Search** box and hit **Go**. If there are many devices satisfying the specified criteria, a list of devices are displayed with their IP Address and category. Click the device whose snapshot you want to view.

The descriptions for various sections of Device Snapshot are as follows:

Device Details: Displays the system's details such as the IP address, operating system, time stamp of previous and next polls and a description on the system hardware details. System description is seen on the SNMP-enabled devices.
Device Notes: This tab shows additional device details. You can add additional fields to denote the device details. Click the  . The added fields are displayed in the snapshot page.

Tools: The following actions can be done by clicking the respective icon:

-  Ping
-  Trace Route
-  Browse
-  Open a Telnet session [Note: Telnet is not enabled in IE7 in Windows and Firefox in Linux. Click here to configure the steps to enable Telnet in IE7 and Firefox.]
-  Open Remote desktop connection [Note: RDP is not enabled in IE7 in Windows. Click here to enable.]

Today's Availability: Displays the device availability of the current day in the form of a pie graph. Click  or  to view the availability report for the past 7 days or 30 days respectively.

Response Time: Shows the current response time of the device. Click  or  to view the response time details for the past 7 days or 30 days respectively. Click  to configure response-time based threshold.

Packet Loss: Shows the packet loss percentage for the device on that day. By default, OpManager sends 1 ping packet during a poll. The ping counts, retries, timeout etc are configurable in the file /conf/Ping.properties.

CPU Utilization: Shows the current CPU load of the device. Clicking the graph shows the trend chart of CPU utilization

Memory Utilization: Displays the current memory utilization of the device.

Disk Utilization: Displays the current disk usage of the device incase of servers.

Monitors: This tab lists different monitors for the device. Select each monitor section to view the monitors. You can add more monitors from the available template, or even remove the unwanted monitors from the device.

Notification Profiles: This tab lists the notification profiles associated to the device. You can add more profiles from here.

Interfaces: Displays the list of interfaces in the selected device with their status and other details. Click the interface name link to view its availability and graphs on traffic and bandwidth utilization.

Actions Menu: List of actions that can be performed on the device include:

- Update Status
- Rediscover Now
- Show Alarms
- Monitoring Interval
- Delete
- Manage/UnManage
- Custom Report

Device Info Menu: The device information that can viewed from this menu include:

- Asset Details- The Hard Disk and RAM details are shown here. More detailed information is shown when integrated with ServiceDesk Plus.
- Installed Software- A list of software installed on the server is shown here and this information is retrieved using SNMP.
- Active Processes- A list of processes up and running in the server is shown and is again retrieved from SNMP.

At a Glance Report: This is a report showing the device health at a glance. It shows details like the availability, response time, packet loss, resource utilizations etc.

Viewing Asset Details

If you have both, OpManager and ServiceDesk Plus running in your network, you can view a detailed asset information of a device, provided the device is discovered in both the applications, and the ServiceDesk settings are configured in OpManager.

To view the Asset Details, select the device and click **Device Info --> Asset Details**. This will show the detailed asset information from ServiceDesk Plus.

If ServiceDesk Plus is not integrated, then make sure SNMP is enabled. The device name, the hard disk size, and the RAM size is gathered for SNMP-enabled devices.

To update these details incase you upgrade your systems, follow the steps given below:

1. Select the device and click **Device Info --> Asset Details**.
2. Enter the values of **RAM size** and **Hark Disk**.
3. Click **Save** to apply the changes.

Viewing Installed Software

OpManager provides you the information on the software installed and currently running on the managed device. You need to have SNMP agent running in the device to view this information.

To view the details, click the device icon in the map. Under **Device Info**, click **Installed Software.**

Viewing Active Processes

OpManager provides you the information on the processes that are currently running on the managed device. You need to have SNMP agent running in the device to view this information.

To view the details, click the device icon in the map. From the snapshot page, under **Device Info** menu, click **Active Processes**.

Configuring Additional Device Properties

Configure additional properties of a device by adding additional fields. This makes device management easy.

1. From **Admin** tab, select **Additional Fields**. A list of pre-populated fields is shown.
2. Select **Device** from **Associate pre-defined fields** to all list-box.
3. Click **Add Field** button on the top right corner of this table and configure the following values.
    1. **Field Name:** Configure the name of the additional property
    2. **Type:** Select the property type
    3. **Field Length:** Set the length of the field.
    4. **Description :** Add a meaningful description for the field.
    5. Click **Save** to apply the configuration.

The properties added is applied to all the devices. The additional fields are displayed when you click the **Device Notes** tab in the device snapshot page. These properties are useful when configuring notification profiles. To delete these fields, select the corresponding check-box, and click the **Delete** link on the top right corner of this table.

Configuring Additional Interface Properties

Configure additional properties of a device by adding additional fields. This makes device management easy.

1. From **Admin** tab, select **Additional Fields**. A list of pre-populated fields is shown.
2. Select **Interfaces** from **Associate pre-defined fields** to all list-box.
3. Click **Add Field** button on the top right corner of this table and configure the following values.
    1. **Field Name:** Configure the name of the additional property
    2. **Type:** Select the property type
    3. **Field Length:** Set the length of the field.
    4. **Description :** Add a meaningful description for the field.
    5. Click **Save** to apply the configuration.

These properties are useful when configuring notification profiles. To delete these fields, select the corresponding check-box, and click the **Delete** link on the top right corner of this table.

Configuring Device Dependencies

The status polling for a device can be controlled based on its dependency on some other device. This prevents the unnecessary status checks made to the dependent nodes.

For instance, many devices will be connected to a switch. If the switch goes down, all the devices connected to it will not be reachable. In this case, it is unnecessary to check the status of the dependent devices.

To configure the dependency for devices, follow the steps given below:

- In the **Admin** tab, under **Configuration**, click **Quick Configuration Wizard**.
- Select **Configure Device Dependencies** and click **Next**.
- Select the category of the device, Router, Switch, Firewall or Server on which the dependency is to be configured. The devices managed under the chosen directory is listed. Choose a device and click **Next**.

Configuring dependencies in individual devices

You can also configure dependencies for a single device from the device snapshot page. Here are the steps:

1. Go to the device snapshot page.
2. From the device details, click the link against the property **Dependency**.
3. Select the device on which it is dependent.

OpManager stops monitoring the devices if the dependent device is down. Configuring dependencies prevents false alarms.

Adding Custom Links to Devices

You might want to access another link either for reference or to another machine in your network over the web (like a VNC to another device for instance). You can add custom links from the snapshot page.

Here are the steps for creating custom links:

1. Go to the device snapshot page.
2. Click Custom Links > Add.
3. Provide a link name
4. Specify the Url that you intend accessing from this device.
5. Associate the link either to that device, or to all devices, or select devices, and save the configuration.

You will now be able to access the links from the snapshot page.

Administratively Disabling an Interface

If you want to administratively disable an interface, it is possible with OpManager in just a few clicks. Here are the steps:

1. Go to the required snapshot page of the interface that you want to disable.
2. Under Interface tab, click the **Disable** button.

The interface gets disabled and the interface's status is changed to Down. To enable the interface again, go to its snapshot page and click the **Enable** button under the Interface tab.

Classifying and Mapping the Devices

Classification and Device Templates

During initial discovery, OpManager categorizes the network devices into servers, printers, switches, routers and firewalls. For proper classification, install and start the SNMP agent on all the managed devices.

OpManager comes with over 600 device templates which carry the initial configurations to classify the devices into the pre-defined categories, and to associate monitors to them. The device templates enables you to effect a configuration once and is applied to several devices at a time whenever there is a change.

The templates carry the information required to classify the devices and to associate relevant monitors. You can define your own templates and modify the existing ones.

Creating/Modifying Device Templates

1. Go to Admin --> Device Templates
2. Click 'New Template' to define a template for a new device type. Click the Template name to modify an existing one.
3. Configure/Modify the following properties:

    - **Device Template**: Specify the device type.
    - **Vendor Name**: Select the vendor. Click **Add New** to add a new vendor, and **Save**.
    - **Category**: Select the category for the device type. On discovery, the devices are automatically placed in the select Category map.
    - **Monitoring Interval**: Configure the interval at which the device needs monitoring.
    - **Device Image**: Select the image for this device type.
    - **System OID**: Type the sysOID and click **Add**. Click **Query Device** for OpManager to query the device for the OID.
    - **Add Monitor**: Click this option to select the monitors.
    - **Edit Thresholds**: Click this option to edit thresholds.
    - Click **Create** button to create the new device template.

The classified devices are placed under different maps for easy management. For proper device classification, make sure you have installed and started SNMP in all the network devices before starting OpManager service.

The default maps include:

- Servers
- Routers
- Desktops
- Switches
- Firewalls
- DomainControllers
- Wireless

- Printers
- UPS

You can also add your own infrastructure views. Custom infrastructure views can be added to group devices which cannot be classified under the default views provided. For instance, if you would like to monitor some IP Phones, it will not be appropriate to classify them as servers or desktops.

This initial classification may not be accurate if

- the network devices do not support SNMP.
- some devices have their SNMP settings different from those specified in the Credential Settings.

Using Interface Templates

Monitoring requirement differs for different interfaces on a device. OpManager allows you to define configuration templates for interfaces of specific types. For instance, the configurations specified for an Ethernet interface can be applied to interfaces of this type across all devices, saving a lot of time.

1. Go to Admin a Interface Templates
2. Click an Interface Template to modify its properties.

The changes are applied to all interfaces of the same type.

Categorization into Default Maps

Devices are categorized into the following default maps in OpManager: The classification is done using SNMP and NMAP.

- Servers
- Routers
- Switches
- Desktops
- Firewalls
- DomainControllers
- Wireless
- Printers
- UPS

The discovered devices are classified into the above categories based on response to SNMP requests sent by OpManager to the devices. The devices that are not SNMP enabled, and the device types which are not included in the template are incorrectly classified under desktop. You can also add your own infrastructure maps to group your devices according to categories, or create business views to logically group devices, for instance, based on geography.

Adding New Infrastructure Views

You can create more defined groups under infrastructure views by adding more custom views. For instance, you might want to group all your Environment Sensors or IP Phones into separate infrastructure views. You can add a new infrastructure view from Maps tab or Custom dashboards.

Adding New Infrastructure View from Maps tab

Here are the steps to add a new infrastructure view from Maps tab:

1. From the pop-up in the Maps tab, click **Add Infrastructure View** option .
2. Specify the category **Name** and click **Add**.
3. From the listed devices, select and move the required devices to this view.
4. Click **Import Now** option.

The selected devices are displayed in the newly created infrastructure views.

Adding New Infrastructure View from Custom Dashboard
OpManager allows you to add a new infrastructure view from the dashboards also, provided if the infrastructure view widget is selected to get displayed in the dashboard. To add a new infrastructure view from the infrastructure widget, follow the steps given below:

1. Click **New Infrastructure View** link available at the bottom of the Infrastructure snapshot widget. Add category window opens.
2. Enter the **Category Name**.
3. Select the category whose properties needs to be inherited for this category.
4. Click **Add** button. Import window opens.
5. From the listed devices, select and move the required devices to this view.
6. Click **Import Now** button to start importing the selected into this category.

After you create new infrastructure views, you can create device templates for devices of this category. This allows you to define monitors specific to the category and automatically applies the configurations defined in the template to the devices as soon as they are discovered.

Sorting Devices in Maps

You can sort the devices on maps by the Name, Display Name, Device Type, or the Severity of the device. This helps you locate a resource faster.

To sort the devices in a map, from the **Sort By** combo-box, select the required option based on which you need the sorting to be done.

Note: Sorting of devices is supported only in the default maps.

Different Types of Map Views

Three different types of views are supported for the default maps. Click the **Select View** combo-box on the top right corner in the **Servers**, **Router**, and **Switches** maps to select the required view type:

1. **Details**: This is a list view of all devices on that map. This is useful when you have a large number of devices on a map.
2. **Large**: This shows bigger device icons, and gives more visibility. For instance, in the Servers map, the device icon also shows a couple of TCP Services monitored on the server indicating the service status. In the Routers and Switches map, all the interfaces are also shown in the map.
3. **Small**: This shows small device icons. The Router/Switch maps show only the parent devices, and in the Servers map, the services are not displayed.
4. **List View**: This list all the devices along with its status, IP Address, CPU & Memory utilized. From here you can apply device template, credentials, notification profiles etc. More.

Import Devices

A few devices are classified into Desktops map even if they are not desktops. This happens when either SNMP is not enabled on the device, or that particular device does not have a device template. You can import these devices into the correct maps as follows.

1. Go to the Map into which you want the devices imported.
2. Click the **Import** button on the top right corner. A corresponding dialog opens.
3. From the **Available Devices** list, select the devices and move them to the **Selected Devices** list.
4. Click **Import Now** to import the devices into the required category.

For instance, if a Router is classified into Desktops, go to the Router map and import the Router.

Managing Users

Create New Users

You can create users in OpManager and provide required privileges to them. The option to create users is available only for the **admin** login account or those accounts which have 'Full Control' privilege. Here is how users are added:

Note: If you have procured a license for a limited number of devices, you can add any number of Users in OpManager. If the license is based on the number of users, you can add only the numbers as allowed in the license.

1. From Admin tab, click User Manager.
2. Click **Add User** option in the User Configuration screen.
3. Configure the following user details:
4. **Login Details**:
   User Name - a user account name
   Password - a password for the above user
   Re-type Password- retype the password for confirmation

5. **Contact Details**:
   Email ID - email ID of the above user
   Phone number: the user's phone number
   Mobile number: the user's mobile number

6. **Access Details**:
   User Permission- Select the permission as **Full Control** to provide complete admin privilege to the user, or select **Read-only Access** to restrict the scope of the user to only read operations. A user with this permission can only view the details.

   Has access to - You can provide this user an access to either **All Devices,** or only specific **Business Views**, and/or **WAN**.

7. Click **Add User** to add the user according to the scope specified here.

Logout and try logging in as the new user and check the privileges.

Changing User Passwords

You can change the password for the users. Either the **admin** user or an user with full control privilege only can change the passwords.

1. Go to Admin --> User Manager.
2. Click the Edit icon against the user name whose password you want changed.
    1. **Password Details**:
       Password - a password for the above user
       Re-type Password- retype the password for confirmation

    2. **Contact Details**:
       Email ID - email ID of the above user
       Phone number: the user's phone number
       Mobile number: the user's mobile number

    3. **Access Details**:
       For users with only partial permission, the business views assigned to that user is displayed. Remove selection for the view if you want to remove the views from the user's purview. For users with full control, this option is not displayed.

Removing Users

You can remover the users.

1. Go to Admin --> User Manager.
2. Click the Delete icon against the user name whose account you want to delete.
3. A confirmation dialog pops up. Click **OK**. The user account is deleted.

Monitoring Network Resources

Monitoring CPU, Memory, Disk Using SNMP

The monitors for CPU, Memory, and Disk Utilization are automatically associated for the devices based on the device template definitions. For instance, for Linux servers, the default template has SNMP-based monitors associated. So, all Linux servers will have SNMP-based resource monitors associated. You will see the dial graphs for these three resources in the device snapshot page if SNMP is enabled.

All the Server templates have the monitors defined for various host resources. By default, the CPU, Memory, and Disk Monitors are associated to the servers. The device snapshot page shows the values of these monitored resources with dial-graphs.

If you do not see these monitors associated to the devices, it could be due to any or all of the following reasons:

- These monitors are not present in the device template.
- SNMP is not enabled on the device. In such case, enable SNMP and add the monitors to the device once again.
- Incorrect SNMP credentials are associated. Check the credential details like the SNMP version, community string etc.

Steps to add the monitors to the device again:

1. From the device snapshot page, select the Monitors tab.
2. From the monitor types, select Performance Monitors.
3. You will see the monitors displayed on the right if associated. Click Add Monitors link on the right.
4. From the list of monitors, select the SNMP monitors for CPU, Memory, and Disk Utilization.
5. You can also add other required monitors like Partition monitors etc.
6. The selected monitors are associated to the device and the resources are monitored.

To check if the SNMP agent in the device returns response, try the following:

1. Click the Edit icon against any of the associated monitor names.
2. From the edit screen, click **Test Monitor** link. This does a dynamic query to the device for the value of the selected resource, and show the data.

Incase the agent does not respond, you see a message to this effect. Refer to the troubleshooting tips to resolve the issue.

As an alternative, you can monitor the non-SNMP Linux servers using CLI (telnet or SSH), or the non-SNMP Windows devices using WMI.

Monitoring Resources Using WMI

OpManager monitors the system resources using SNMP by default. However, in the absence of SNMP on the devices, the non-SNMP windows devices can be monitored using WMI. All the Windows device templates have the resource monitors preconfigured. All you will need to do is, disable the SNMP monitors associated and select the WMI monitors and associate them to the required devices.

Prerequisites

For monitoring the Windows environment, OpManager must necessarily be installed on a Windows machine. Besides, the device where OpManager is installed and the monitored remote Windows devices must have WMI, RPC, and DCOM services enabled on them. Authentication to the remote devices using WMI requires you to login as a domain user with administrator privileges. This is a requirement of the WMI protocol. If the device is in a workgroup, the system user name and password should suffice.

Steps to configure WMI Monitoring

Go to the device snapshot page.

1. From Monitors --> Performance Monitors section, remove the SNMP-based monitors if any.
2. Click Add Monitors link on the right bottom.
3. Now, from the list of resource monitors, select the CPU, Memory, and Disk Utilization monitors which has the protocol name as WMI against the monitor name.
4. Click OK. The monitors are added in the template under the Monitors column.
5. Click Apply. All the Windows devices to which the monitors are associated are listed. Another column also displays devices which are classified as 'Unknown'. You can pull the required devices from this list too. Click Apply once again.

The WMI-based monitors are associated to the device.

Monitoring Resources Using CLI

OpManager monitors the system resources using SNMP by default. However, in the absence of SNMP on the devices, the non-SNMP Linux devices can be monitored using CLI, ie., Telnet or SSH.. All the Unix Servers templates have the resource monitors preconfigured. All you will need to do is disable the SNMP monitors associated and select the CLI monitors and associate them to the required devices.

Prerequisites

For monitoring the unix servers, make sure either Telnet or SSH is enabled on them.

Steps to configure Telnet/SSH Monitoring

Go to the device snapshot page.

1. From Monitors --> Performance Monitors section, remove the SNMP-based monitors if any.
2. Click Add Monitors link on the right bottom.
3. Now, from the list of resource monitors, select the CPU, Memory, and Disk Utilization monitors which has the protocol name as CLI against the monitor name.
4. Click OK. The monitors are added in the template under the Monitors column.
5. Click Apply. All the servers to which the monitors are associated are listed. Another column also displays devices which are classified as 'Unknown'. You can pull the required devices from this list too. Click Apply once again.

The CLI-based monitors are associated to the device.

Adding More Monitors

Following are the monitors associated by default for the different device categories:

- **Servers**: CPU, Memory, Disk Utilization
- **Routers**: CPU, Memory, Buffer Hits/Misses, Temperature
- **Switches**: CPU, Memory, BackPlane Utilization
- **Firewalls**: CPU, Memory, and Connection Count.

Similarly, other categories also have few resources monitoring triggered by default. Besides the ones automatically associated, you can monitor more parameters. Here are the steps to configure more monitors:

1. From Admin, select Device Templates.
2. From the list of templates, select the template for the device type to which you want to associate more monitors. Select the corresponding letter to get to the template quickly.
3. In the device template, from the **Monitors** column, click the **Add Monitor** button.
4. All the predefined monitors are listed. Select the required monitors from here and click OK.
5. All the devices of the same type are listed. Click Apply for the selected monitors to be associated to all the selected devices.

Adding Custom Monitors

In addition to OpManager's default monitors, you can also create your own monitors for the SNMP-enabled devices in your network. The SNMP variable for which you intend configuring a monitor can return either a numeric or a string output when queried.

To add a custom monitor for a resource of a particular device type, the device template must be modified. The new monitor should be defined in the device template so that the monitor is associated for all devices of that type. Here are the steps.

1. Go to **Admin** --> **Device Templates**.
2. Select the template in which you want to add a new monitor. Eg: Linux. Click the letter L to displays templates starting with this letter.
3. From here, click any template. Example - Linux. Scroll down the template and click **Add Monitors** under Monitors column.
4. Click the **New Monitor** link in this page.
5. Click the **Select** button in the Add a new monitor page to browse and select the OID for which you want add a monitor. The MibBrowser is shown.
6. Load the required MIB and select the OID. Eg: hrStorageSize from HostResource MIB. Click **OK** after selecting this OID.
7. Configure all the other properties of the monitor like the name, display name, units etc. Click **OK**. The new custom monitor is listed under Monitors column in the template.
8. Click **Apply**.
9. The devices are listed prompting you to select the devices for which you want the monitor to be associated. Check the list of devices and click **Apply**.
10. The modified template is applied to all devices of type Linux. Go to the snapshot page of any of the Linux devices. You will find the new custom monitor in the list of associated performance monitors.
11. For SNMP-based monitors to work, make sure to enable SNMP on the devices and check if the OID is implemented.
12. To easily apply a new monitor to a set of devices, you must add the monitor to the device template.

Consider the example given below to add a custom monitor that monitors a SNMP variable which returns a string output when queried.

1. Go to the **Linux template** page.
2. Click on **Add Monitor**s under Monitors column.
3. Click on **New Monitor** in the Add Monitors page,
4. Click on **Select** button in order to open the MIB browser.
    1. Select **RFC 1213** MIB and click on **Expand All** .
    2. Choose the **System Name** variable. The OID of it will be displayed at the bottom. [This variable will give the System Name of the device when queried].
    3. Click on **OK**. The OID will be displayed in the SNMP OID field.
5. Configure all the other properties of the monitor like the name, display name, units etc. Click **OK**. The new custom monitor is listed under Monitors column in the template.
6. Click on **Apply** to add the template to the devices.
7. The devices are listed prompting you to select the devices for which you want the monitor to be associated. Check the list of devices and click **Apply**. The monitor will be associated to the selected devices under performance monitors.

Device-specific Monitors

The monitoring configuration may need alteration for specific devices. Doing a bulk-configuration using the device templates, applies the same set of configurations for the devices of the same type. In order to change the configuration for specific devices, here are the steps:

1. Go to the device snapshot page.
2. Scroll down to the Monitors section.
3. From here select the required monitors. Monitors of the selected category are listed on the right.
4. Click the Edit icon against the monitor name. The Edit Monitor page is displayed.
5. Change the values for the required parameters and and click OK.

The changes to the monitor are effected only for that device.

Configuring thresholds for monitors

Configuring thresholds enable OpManager to proactively monitor the resources and the services running on them and raise alerts before they go down or reach the critical condition. You can configure thresholds for the monitors that are associated to a single device, configure from the device template in order to apply across multiple devices and also configure from Quick Configuration Wizard.

Configure threshold limits for the monitors associated to a single device

1. Go to the device snapshot page.
2. Under Monitors tab, click on the edit icon corresponding to the monitor for which you want to configure threshold limits. Edit Monitor page opens.
3. Ensure that the **SNMP OID** and the monitoring **Interval** are configured.
4. Select the **Threshold Alert** condition [>,= or <] and enter the value. Alert is raised if the monitored value is greater than, equal to or lesser than (which ever is selected) the threshold value.
5. Enter the **Rearm Value**. Rearm value is the value which the determines the monitor has restored to normal condition. For instance, the threshold condition for a memory monitor is selected as greater than [>] and the threshold value is configured as 75. The monitored memory value of that device is 80. Now alert is raised and the monitor is in violated condition. At the next poll the monitored value is 72. An alert for returning to normal condition is generated. At the next poll again the monitored value goes to 80. Again a threshold violation alert is generated. In order to avoid this, enter the rearm value. Only if the monitored value reaches the rearm value the monitor goes to the normal condition and a normal alert is raised. Note: If you select threshold condition greater, then the rearm value should be lesser than the threshold value and vice versa.
6. In the **Consecutive Times** field enter the value of how many consecutive times the threshold can be violated to generate the alert.
7. Click on **Advanced** button to configure the Alarm Message and Severity. Based on the monitor, the values for Alarm message and severity are pre-configured by default.
8. Click on **OK**.

Configure threshold limits for the devices from their device template page

1. Go to the Device template page.
2. Under **Monitors** tab, all the monitors that are currently associated with the devices are listed. If you want add or remove required monitors. Click on **Edit Threshold** button. Edit Thresholds page opens.
3. Configure the Threshold Alert and Rearm Value and click on **OK**.
4. Click on **Apply**.
5. Select the devices for which you want to associate the monitors from the left column and move to the right column.
6. Again click on **Apply**.

Configure thresholds for multiple devices from Quick Configuration Wizard

1. From **Admin** page, click on **Quick Configuration Wizard**.
2. Select **Add Performance monitors to several devices (SNMP, WMI and CLI)** option and click on **Next**.
3. Open the required device template page and follow the steps from 2 to 6 of Configure thresholds for the devices from their device template page.

Viewing Process Diagnostics

You can view the top ten processes utilizing the maximum resources. Process statistics is retrieved using Telnet/SSH/WMI, for which the correct credential must be associated to the devices. To be able to view the diagnostics,

1. Configure relevant CLI and WMI credentials.
2. Click the  link on top of the dial graphs for CPU, Memory, and Disk graphs. The top 10 processes are shown.

You can also end the processes from here.

Viewing Live Workload on CPU, Memory and Hard disk

OpManager provides you the option to view the workload handled by the CPU, Memory and Hard disk of a device in real time. This option is very useful in cases where you would have restored a device just a short time back and want to continuously monitor for few minutes. To view the live workload,

1. Go to the device snapshot page.
2. Click on the Real Time icon  available on top of the CPU, Memory and Hard disk dials to view the live workload.

The amount of CPU/Memory/Hard disk that is being currently utilized by the device is displayed in a graph in terms of percentage for the configured Refresh Interval and Time Window.

Viewing Live Interface Traffic

OpManager provides you the option to view the traffic handled by an interface in real time. Here are the steps:

1. Go to the device snapshot page.
2. Click on **Interfaces** tab. All the interfaces of the device gets listed.
3. Click on the respective Real Time icon  of the interface whose live traffic has to be viewed.

Live In and Out traffic in the interface is displayed as a graph for the configured Refresh Interval and Time Window.

Viewing Live Temperature

OpManager provides you the option to view the temperature of the router in real time. Here are the steps:

1. Go to the snapshot page of the router.
2. Click on the Real Time icon  available on the temperature value that is displayed.

Live temperature of the router is displayed as a graph for the configured Refresh Interval and Time Window.

Modifying Live View Parameters

Live View displays the resources utilized, temperature and traffic details as a graph for the configured Refresh Interval and Time Window. Refresh Interval determines the interval between successive polls to the resource and the Time Window determines the period for which the data has to be displayed continuously. By default the Refresh Interval is 1 second and the Time Window is 5 minutes. To modify the default Refresh Interval and Time Window values, follow the steps given below:

1. In the Live view window, click the **Configure** button.
2. Enter the required value in the **Refresh Interval** and **Time Window** fields.
3. Click **Modify** to effect the changes.

Monitoring Packet Loss for Devices

You can monitor the packet loss percentage on a per device basis and view even the packet loss reports.

1. Go to the device snapshot page.
2. Look at the **Today's Packet Loss** value shown on the right.
3. Click the corresponding small icons to see the packet loss report for the last 7 or 30 days.
4. Click the  icon to configure threshold value in percentage. If the packet loss percentage exceeds the threshold value, a threshold violation alarm is triggered. This alarm can inturn be notified.

Monitoring Response Time of Devices

You can monitor the response time on a per device basis and view even the packet loss reports.

1. Go to the device snapshot page.
2. Look at the **Response Time** value shown on the right to know the device response time..
3. Click the corresponding small icons to see the response time report for the last 7 or 30 days.
4. Click the  icon to configure threshold value in milliseconds. If the device response time exceeds the threshold value, a threshold violation alarm is triggered. This alarm can inturn be notified.

Monitoring TCP Services

OpManager provides out-of-the-box support for the following services: Web, HTTPS, FTP, IMAP, LDAP, Telnet , MySQL, MS-Exchange, SMTP, POP3, WebLogic, Finger, Echo, DNS, and NTTP. By default, during discovery, OpManager scans the devices for the services: DNS, MSSQL, MySQL, Oracle, SMTP, Web. You can also select other services in the list. When they are found running on their default ports, OpManager starts monitoring the services.

Scanning Services during Discovery

By default, OpManager scans each device on the network for the services that are chosen during discovery.
To modify this list, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Discovery**, click **Services**.
3. Select the check boxes under **Scan during discovery?**, corresponding to the services to be discovered and clear the selection for the services that are not to be discovered.
4. You can modify the service monitor properties in OpManager. When the service is not running on the default port, you can configure the actual port in which it is running, and you can change the timeout interval. **Save** the changes.
5. Click **Update** to apply the changes.

OpManager allows you to change the settings for monitoring these services as per your network needs. You can configure new services that are not available in the list. OpManager can manage services running on standard TCP ports.

Note:

- The list contains the service names and the corresponding port numbers. To edit the settings of any of the available services, click Edit icon.
- If you do not find the service you want to manage in the list, you can add the service by clicking **Add Service** under **Actions** menu. For details, refer to Adding a New Service.

Viewing Service Status and Response Time

1. Go to the device snapshot page.
2. Under **Service Monitors**, you will see the list of services managed in the device, if any, with their status and current response time.
    - Click the service name to view the historical report on the response time and the availability chart of the service.
    - Click the Availability chart to view the service downtime/uptime chart, summary and historical information.

Monitoring TCP Services on a Device

To select the services to be monitored in a device, follow the steps given below:

1. Click the Server in the map.
2. In the Monitors section, select **Service Monitors** to see the monitors listed.
3. Click **Add Monitor** at the bottom of this list to see the complete services list..
4. Select the services to be discovered from the list and click **OK**.

Adding New TCP Service Monitors

You can add new TCP services for monitoring.

1. Go to Admin --> Services Monitors
2. From the Actions menu in this screen, select **Add Service**.
3. Specify the name of the TCP service that you want to monitor.
4. Specify the TCP Port number that has to be checked for service availability
5. Specify the timeout interval in seconds for the port-check request.

Associating the Service to Devices

To associate a service to a server,

1. Go to Admin --> Service Monitors
2. From the Actions menu, select **Associate**.
3. Select the required TCP service from the list of services displayed.
4. Select the devices on which you want to monitor the service from the column on the left and move them to the right.
5. Click Save.

Using Quick Configuration Wizard

You can also use the Quick Configuration Wizard to associate a service to several devices at one go. Here are the steps:

1. From the Admin tab, select Quick Configuration Wizard.
2. Select the option **Add a new service monitor to several devices** and click Next.
3. Now, select **Associate a service to servers** option and click Next again.
4. All the available TCP services are listed. Select the service which you want to monitor on your servers. Click Next.
5. Select the devices on which you want to monitor the service from the column on the left and move them to the right.
6. Click Finish. The service monitor is associated to the selected devices.

Monitoring Windows Services

Certain applications in Windows machine run in the background as services. OpManager discovers and monitors the status of such services using WMI. OpManager generates alarms whenever they fail.

Prerequisites

To monitor Windows services, OpManager should be installed in a Windows machine. OpManager uses WMI to monitor the Windows services and hence you need to provide the log on details of a user with administrative privilege to connect to the device. So, make sure you configure a WMI credential so that you can apply this to the windows devices.

Associate Windows Services to a Device

To monitor a Windows service, follow the steps given below:

1. Go to the device snapshot page.
2. Confirm if the correct WMI credential is associated to the device. Else, configure the password details in the device.
3. Click **Add Monitor** in the **Windows Service Monitors** section. This option will be available only for Windows servers.
4. Select the services to be monitored in the device and click **OK**.

Associate Windows Service Monitors to several devices

From the Admin tab, select Windows Service Monitors.

Select **Associate** option from the Actions menu.
From the drop-down list box, select the services one-by-one and move the devices from the 'not monitored' column to the 'monitored' column.
Click Save.

The selected service monitor is added to the device.

Using Quick Configuration Wizard

You can also use the Quick Configuration Wizard to associate a service to several devices at one go. Here are the steps:

1. From the Admin tab, select Quick Configuration Wizard.
2. Select the option **Add a new service monitor to several devices** and click Next.
3. Now, select **Associate a Windows service** option and click Next again.
4. All the available Windows services are listed. Select the service which you want to monitor on your servers. Click Next.
5. Select the devices on which you want to monitor the service from the column on the left and move them to the right.
6. Click Finish. The service monitor is associated to the selected devices.

Adding New Windows Service Monitors

In addition to the Windows services monitor supported by OpManager out-of-the-box, you can add monitors for other windows services too..

To add a new Windows service monitor, follow the steps given below:

1. Under the **Admin** tab, click **Windows Service Monitors**.
2. Under **Actions**, click **Add Service**.
3. Type the name of the device in the **Device Name** field.
4. Type the domain administrator user name password for the device in the respective fields and click **Next**.
5. A list of all the Windows Services available on that machine is displayed. From this select the services that you want monitored across all other Windows Servers.
6. Based on whether or not you want to restart the service or the machine when the service goes down, select the corresponding option.
7. Click **Finish**. A list of Services for which a monitor is added is shown.
8. Click the link at the bottom of this list to associate these service monitors to devices.
9. From the drop-down list box, select the services one-by-one and move the devices from the 'not monitored' column to the 'monitored' column.
10. Hit **Save**.

The newly added services are also monitored on the selected servers.

Monitoring Processes on Windows/Unix Servers & Desktops

OpManager provides out-of-the-box support for monitoring the availability of all the processes running on a Windows or Unix system. Windows systems uses WMI and Unix systems uses CLI to monitor the processes that are running on the system.

Here are the steps for configuring Process Monitors:

1. Go to the device snapshot page.
2. Make sure you have associated the WMI/CLI Credentials to the device.
3. From the Monitors tab, click on **Process Monitors**.
4. Click on the relevant link on Process Monitors column on the right and select the required processes to be monitored.
5. Click OK to associate the monitors to the device.

Configure Thresholds for Process Monitors

You can set resource thresholds for the Process Monitors. Once a resource (cpu/memory) utilization by a process exceeds the configured threshold, an alert is triggered.

1. Click the Edit icon against the process name.
2. Configure the threshold values for CPU and Memory resources.
3. Configure the number of times you would like to allow threshold violation before being notified. For instance, if you configure the value as 3, OpManager notifies you if the resource threshold is violated 3 consecutive times.
4. Configure the number of the process instances, exceeding which you would like to be notified. For instance, if you would like to be notified if the number of Apache.exe instances on the monitored device exceeds 3, configure the value here as 3 and save the changes.

Alerts are fired based on the above settings.

You can also view active processes on a device and also view the process diagnostics against a system resource.

Adding New Process Template

Process templates helps you to select the processes that are running on a device, convert each of them into individual templates and apply all of them across multiple devices. To add a new process template,

1. Go to **Admin**-> **Process Templates**.
2. Click **Add New**. Add New Template window opens.
3. **Device Name**: Select the device which runs the process(es) that needs to be converted into template(s).
4. **Protocol**: Select the relevant protocol to access the device.
5. Configure the correct credentials. Note: If new credential settings have to be configured, then click **New** button.
6. Click **Next**. All the processes that are currently running on the device are listed along with their ID, Path and Arguments.
7. Select the required process(es).
8. Click **Add**. Associate process Template Window opens.
9. From the listed devices, select and move the required devices.
10. Click **Associate**.

The selected processes are converted into templates and associated across multiple devices.

Associating Process Template to Multiple Devices

To associate a process template across multiple devices, follow the steps given below:

1. Go to **Admin**-> **Process Templates**.
2. Click **Associate**.
3. Select the process template to be associated to multiple devices,
4. From the listed devices, select and move the required devices.
5. Click **Associate**.

The selected process template is applied across multiple devices.

Monitoring VMware ESX Using OpManager

VMware ESX server hosts multiple server instances on a single host machine. Each instance functions as an individual server component and can host applications. The server instances on the VMware ESX can have different OS and each instance is monitored by OpManager for availability and performance. Using OpManager, you can monitor the entire VMware ESX server unit and also each instance within for clear visibility into its performance, the monitored versions being ESX version 3 or higher.

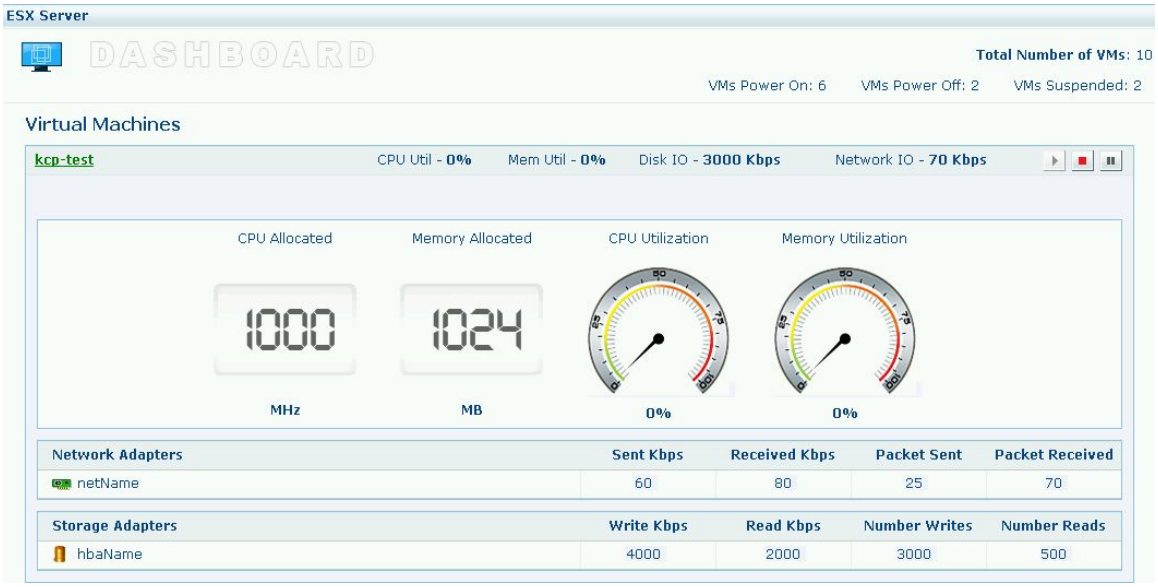
Availability & Performance: Besides monitoring the availability of the VMware and its individual instances, you can also closely monitor the performance of the resources on each instance like the CPU, Memory, and if the allocated resource for each instance is utilized optimally. Intuitive dashboard graphs for the server farm helps you quickly identify if the resources are over-utilized or under-utilized.

Capacity Planning: Having a VMware in your production environment helps in capacity planning and in effective use of the system's resources. OpManager aids you in optimizing productivity by monitoring the availability of resources on the host. It is also that your server's capacity is very much under-utilized. A snapshot view of the VMware in OpManager, helps in quick decision making and levering the resources optimally.

Steps to configure VMware ESX Server Monitoring

1. Configure the required SNMP Credential for the ESX Server.
2. Discover the device in OpManager. The device is discovered and classified as ESX Server.

Besides the CPU, Memory, and Disk dial graphs, you will also find a dashboard report for all the virtual machines on the ESX Servers. Here is a screenshot of the dashboard:



Following are the parameters shown in the dashboard:

- The number of virtual machines on the ESX server
- The status of each of the VMs (powered on, off, or suspended)
- The allocated system resources (CPU & Memory) for each VM
- The used percentage of resources on each VM
- The Disk I/O and Network I/O
- The CLI-based monitors are associated to the device.

Active Directory Monitoring

Active directory monitoring feature takes OpManager a step further in proactive monitoring of Windows environment. The system resources of the Domain Controllers where the Active Directory (AD) database resides, and few critical Active Directory Services are monitored in OpManager.

To make AD monitoring more simple and easily accessible, The Domain Controllers are classified under a separate category under Infrastructure Views. The categorization of the device as a Domain Controller is done automatically if SNMP is enabled. The system resources of the device and the AD services are monitored using WMI.

The snapshot page of the Domain Controller shows a dial graph for AD Store in addition to the dial graphs for CPU, Memory, and Disk Utilization.

The other utilization data displayed in the snapshot page for the Domain Controller are:

- Resource Utilization by LSASS (Local Security Authority Subsystem Service)
- Resource Utilization by NTFRS (NT File Replication Service)
- Ad Store Utilization
- Performance Counters showing information such as the AD Reads, the AD Replication objects etc

Besides these, following are the AD Services monitors associated by default:

- **Windows Time service** : The service synchronizes the time between domain controllers, which prevents time skews from occurring.
- **DNS Client Service** : This service resolves and caches (Domain Name Server) DNS names.
- **File Replication Service** : This service maintains file synchronization of file directory contents among multiple servers.
- **Intersite Messaging Service** : This service is used for mail-based replication between sites. Active Directory includes support for replication between sites by using SMTP over IP transport.
- **Kerberos Key Distribution Center Service** : This service enables users to log on to the network using the Kerberos version 5 authentication protocol.
- **Security Accounts Manager Service** : This service signals other services that the Security Accounts Manager subsystem is ready to accept requests.
- **Server Service** : This service enables the computer to connect to other computers on the network based on the SMB protocol.
- **Workstation Service** : This service provides network connections and communications.
- **Remote Procedure Call (RPC) Service** : This service provides the name services for RPC clients.
- **Net Logon Service** : This service supports pass-through authentication of account logon events for computers in a domain.

You can add more AD Monitors to be monitored by clicking the Add Monitor button.

Exchange Server Monitoring

You can monitor critical MSExchange 2000/2003 Services and parameters using OpManager. Monitoring is done using WMI. Thresholds are pre-configured for critical services. You can also modify or enable thresholds for other services and parameters.

The services monitored are:

- Information Store
- Site Replication Store
- MTA Stacks
- Exchange Management
- SMTP
- POP3
- IMAP4
- System Attendant
- Routing Engine
- Event Service

The Exchange parameters that are monitored can be classified under the following categories:

- Address List Monitors
- POP3 and IMAP Monitors
- Information Store Public Folder Monitors
- Event Service Monitors
- SMTP Monitors
- Information Store Mailbox Monitors
- Message Transfer Agent Monitors
- Directory Service Monitors
- Information Store Monitors

Configuring Exchange Parameters and Services Monitoring

1. Go to the snapshot page of a device that has Exchange running.
2. Scroll down and select the **Monitors** tab.
3. Click on **Performance Monitors**. The monitors are listed on the right.
4. Click the **Add Monitor** button on the right. A list of monitors is displayed.
5. Click the **Exchange Monitors** button on top of this list. The monitors of all the Exchange parameters and services are displayed.
6. From this list, select the required Monitors and associate it to the Server.

These monitors are associated to the device. Ensure to associate the correct WMI credential to the device. OpManager uses these credentials to connect to the device using WMI.

Monitoring MSSQL Parameters

MSSQL Services and Parameters can be monitored using WMI. Here are the steps to associate the MSSQL monitors to a device:

1. Go to the snapshot page of a device that has MSSQL running.
2. Scroll down and select the **Monitors** tab.
3. Click on **Performance Monitors**. The monitors are listed on the right.
4. Click the **Add Monitor** button on the right. A list of monitors is displayed.
5. Click the **MSSQL Monitors** button on top of this list. The monitors of all the MSSQL parameters are displayed.
6. From this list, select the required MSSQL Monitors and associate it to the Server.

These monitors are associated to the device. Ensure to associate the correct WMI credential to the device. OpManager uses these credentials to connect to the device using WMI.

Monitoring Windows Event Logs

The Event Log is a Windows service that logs about program, security, and system events occurring in Windows devices. The events can be related to some application, system or security. You can monitor these events using OpManager and configure to generate alarms when critical events are logged. OpManager uses WMI to fetch the details of these logs and hence you need to provide the log on details of a user with administrative privilege to connect to the Windows machine.

You can view the list of all events monitored by OpManager, by clicking **Event Log Rules** under the **Admin** tab.

Monitoring Windows Events in a Device

To monitor Windows events, you need to associate the event log monitors with the device. To do so, follow the steps given below:

1. Go to the device snapshot page.
2. From the **Actions** menu, click **Event Log Rules**.
3. Select the event logs to be monitored in the device.
4. Change the **Polling Interval** if necessary. During each poll, the selected event logs are compared with the events logged in the device and for the matching events, alarms are generated.
5. Click **Save** to save the changes.

Using the Quick Configuration Wizard

Alternatively, you can associate an event log rule with many devices at a time using Quick Configuration wizard.

1. From the Admin tab, select Quick Configuration Wizard.
2. Select the option **Associate Event log rules to several devices** and click Next.
3. Select the log file from the displayed list.
4. Select any one rule from the list of rules shown. Click Next.
5. Select the devices on which you want to monitor the event logs from the column on the left and move them to the right.
6. Click Finish. The event log monitor is associated to the selected devices.

Creating an Event Log Monitor

To create an event log monitor, follow the steps given below:

1. Under the **Admin** tab, click **Event Log Rules**.

   In this page, you can see the rules supported by OpManager. They are categorized into Applications, Security, System, DNS Server, File Replication Service, and Directory Service. You can add the event logs that you want to monitor under any of these categories.
2. Click **New Rule** under any one of the categories to add a rule in it.

   Entries to all the fields except Rule Name are optional. Event ID is a required field to identify the event but can be left empty in few exceptional cases, such as you want to monitor all events that are of the Event Types, say, error or information. Here the filter will be based on the Event Type.
   - Type a unique **Rule Name**.
   - Enter the **Event ID** to be monitored. This is the unique identifier for the event logs.
   - Enter the event **Source**. This is the name of the software that logs the event.
   - Enter the event **Category**. Each event source defines its own categories such as data write error, date read error and so on and will fall under one of these categories.

- Type the **User** name to filter the event log based on the user who has logged on when the event occurred.
- Choose the **Event Types** to filter the event logs based on its type. This will typically be one among Error, Warning, Information, Security audit success and Security audit failure.
- Enter the string to be compared with the log message. This will filter the events that contains this string in the log message.
- Choose a severity for the alarm generated in OpManager for this event.

3. Click **Add Rule** to save the event log rule.

You can now associate this rule to the required devices.

Monitoring URLS for Availability

You can configure OpManager to monitor your Web sites. Many business enterprises require continuous monitoring of their Web sites, as the failure of these sites might have an impact on the business.

You can monitor global URLs, such as www.yahoo.com and www.adventnet.com or URLs in a server, such as http://192.168.4.11/index.html, http://web and so on.

You can perform a content match on these URLs and confirm their availability. Further, for pages that require a form submit, such as user name and password, you can provide these details and verify the availability of the next page.

Note: If a proxy server is configured in your network, make sure to provide its details in the Proxy Server Settings page of OpManager. Refer to Configuring Proxy Server Settings for steps to do this. This is required for monitoring any URL in a proxy-enabled LAN.

To configure a global URL monitor, follow the steps given below:

1. Under the **Admin** tab, click **URL Monitors**. In this page you can add, edit, and delete the URL monitors.
2. To add a URL monitor, click **Add URL**.
3. Enter a name to the URL monitor in the **URL Monitor name** field.
4. Type the **URL address** to be monitored.
5. Type the **Monitoring Interval** and the value of **Timeout** in the respective fields.
6. Enter the Email ID in the **Send Alert to** field to be notified when this URL goes down.
7. Type the string to be compared with the contents of the monitored Web page.
8. Select between **Get** and **Post**, the methods for any HTTP/HTTPS-based URLs. This is required because certain URLs cannot be accessed using a Get request.
9. Type the request parameters and their values in the form <parameter name>=<value>, if any, to know the actual availability of the URL. Note that you can enter only one parameter in a line.
10. Configure the user name and password for authorization. This will be required in the pages where you need to log-on and test the availability of the host.
11. Click **Check Now** to check the availability of the URL based on the given details. You can verify the correctness of the given details using this instant check.
12. Click **OK** to add the URL monitor.

Viewing URL Response Time and Availability

You can get the details about the URL response time and availability in the URL snapshot page.

To view the URL snapshot, click the URL link in the Home page or Maps tab. Then click the URL whose snapshot you want to view.

Click the Availability chart to view the availability history and the URL downtime/uptime chart.

Associating URL Monitors to Servers

You can add URL monitors to Servers to check the availability of the URL from those servers.

1. Go to the device snapshot page.
2. Scroll down to the Monitors section and click URL Monitors.
3. On the right, you will find a link to add the monitors. Click to add monitors
4. Configure all the values for the URL Monitor.

The configured URL is monitored for availability from that Server. You can configure to receive an e-mail or SMS when the URL monitored in a server goes down. For this, you need to create a notification profile for the 'URL is down' criteria and associate it to the server.

Adding Syslog Rules

Syslog is a client/server protocol that sends event notification messages to the syslog receiver. These event notification messages (usually called as syslog messages) help in identifying the authorized and unauthorized activities like installing software, accessing files, illegal logins etc. that take place in the network. In OpManager Syslog rules helps in notifying you if some particular syslog messages such as kernel messages, system daemons, user level messages etc. are sent by the devices.

Apart from the pre-defined syslog rules you can also add any number of syslog rules. Here are the steps to add a syslog rule:

1. Go to **Admin**-> **Syslog Rules**.
2. Click on the **Actions** drop down menu and select **Add New Rule**. Add Syslog Rules window opens.
3. Enter a unique **Rule Name**.
4. Enter a brief **Description** about the rule.
5. Select a **Facility**. Facility refers to the application or the OS that generates the syslog message. By default "Any" is selected.
6. Select the required **Severity**.
7. Enter the text that needs to be verified for matching. Note: Regex is supported for this field.
8. Select the **Alarm Severity**.
9. Enter the **Alarm Message**.
10. Click the **Advanced** button to configure advanced (threshold) rules. This is optional.
    1. **Number of Occurrences**: Enter the count of the number of consecutive times OpManager can receive syslog message from a device before raising an alert.
    2. **Time Interval (seconds)**: Enter the time interval that should be considered for calculating the number of occurrences.

    To clear or rearm the event:
    3. Select the **Facility Name**.
    4. Select the **Severity**.
    5. Enter the **Matching Text**.
    6. Click **Save**.
11. Click **Save**.

Configuring Syslog Ports

OpManager receives the syslog packets via the default syslog port 514. However, if required you can configure additional ports in OpManager to receive the syslog packets. To configure additional ports, follow the steps given below:

1. From **Admin** tab, click **Syslog Rules**.
2. Click on the **Actions** drop down menu and select **Syslog Port**.
3. Enter the port number(s) separated by a comma.
4. Click **OK**.

Monitoring Syslog Packets

Syslog viewer allows you to ensure whether OpManager receives the syslog packets sent by the devices. Here are the steps to view the list of the devices that send the syslog packets:

1. From **Admin** tab, click **Syslog Rules**.
2. Click on the **Actions** dropdown menu and select **Syslog Viewer**.

The syslog packets sent by the devices to OpManager are listed. You can also filter the syslog packets by device and port.

Filtering Syslog packets

1. Enter the device's IP address in the **Source IP field**.
2. Enter the **port** number via which OpManager receives the syslog packets.

Viewing Syslog Flow Rate

To view the flow rate of the syslog packets,

1. Go to **Admin**-> **Syslog Rules**.
2. Click on the **Actions** dropdown menu and select **Flow Rate**.

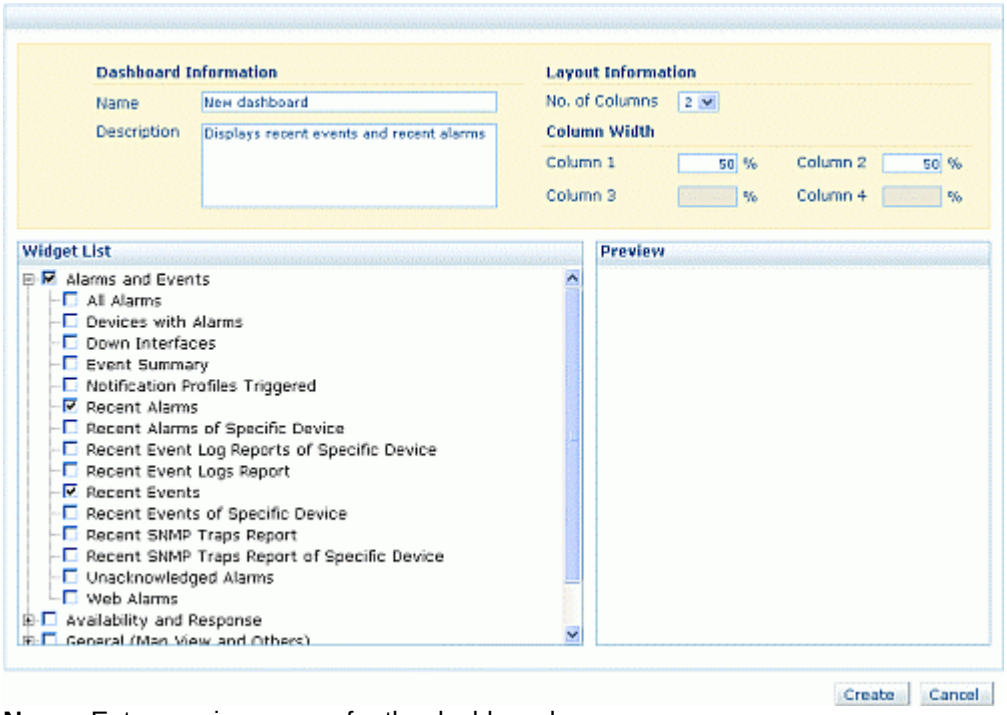
The flow rate of the Syslog packets are displayed.

Customizing Dashboards

Create New Dashboard

Customizing Dashboard feature in OpManager helps you to create your own dashboard and view the desired performance metrics, reports etc at-a-glance. To create a New Dashboard follow the steps given below:

1. From **Dashboards** tab, click on **Action** drop down menu and select **New Dashboard**. Create New Dashboard window opens [screen shot given below].



2. **Name**: Enter a unique name for the dashboard.
3. **Description**: Brief description about the dashboard.
4. **No. of Columns**: Select the number of columns that you want to have in the dashboard. By default the number of columns is 2.
5. **Column 1, Column 2, Column 3 & Column 4**: Enter the width of the columns in terms of percentage.
6. **Widget List**: Select the Widgets that are to be displayed on the dashboard.
7. **Preview**: Displays the preview of the dashboard.
8. Click **Create** button.

A new dashboard is created and listed under the Dashboard drop down menu that is available in the Home page.

Adding New Widgets

To add a new widget to a dashboard follow the steps given below:

1. Mouse-over **Dashboards** tab and click on name of the **Dashboard** to which you want add widgets.
2. Click on **Actions** drop down menu and select **Add Widgets**.
3. Select the Widget(s) that you want add to the dashboard.
4. Click **Add** button to add the selected widget(s) to the dashboard.

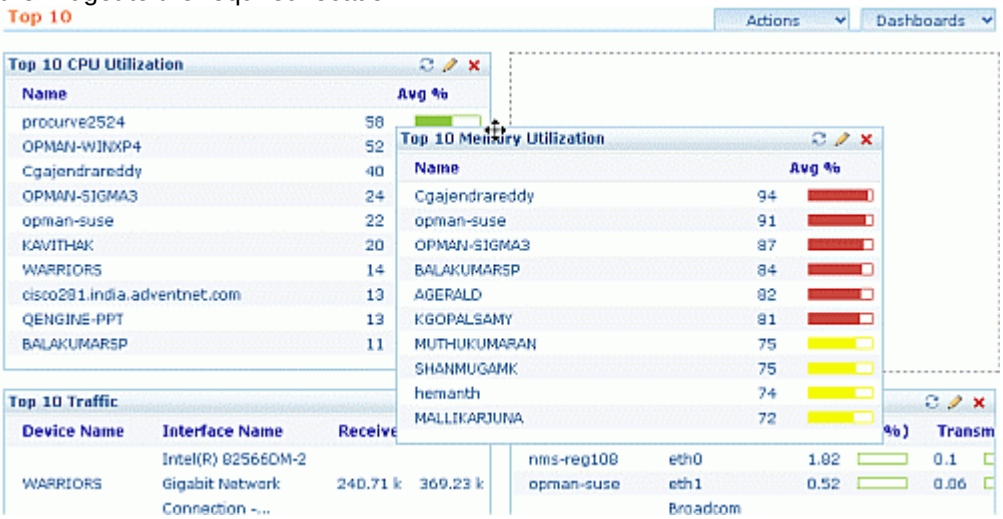
Editing Widgets

To modify the existing widgets go through the steps given below:

1. Click on **Edit Widget** icon  available on the widget box. Edit Widget window opens.
2. Modify the required fields.
3. Click **Submit** to effect the changes.

Moving Widgets

OpManager allows you to move the widgets to different locations within the dashboard. To move a particular widget to a different location, click on the widget name (without releasing the click) and drag the widget to the required location.



The widget is now moved to the new location. The widget that is near the old location occupies the old location automatically.

Deleting Widgets

To delete a widget go through the steps given below:

1. Click on **Delete Widget** icon ✖ available on the widget box. A confirmation window pops up.
2. Click **OK** to confirm deleting.

Setting a Custom Dashboard as the Default Dashboard

To set a custom dashboard as your default dashboard, follow the steps given below:

1. Mouse-over **Dashboards** tab and select the **Dashboard** which you want to set as the default dashboard.
2. Click on **Actions** drop down menu and select **Set as Default**.

The dashboard will be displayed whenever you log-in to OpManager or access the Dashboards tab.

Editing Dashboard Layout

To modify the existing dashboard layout follow the steps given below:

1. Mouse-over **Dashboards** tab and select the **Dashboard** whose layout has to be changed.
2. Click on **Actions** drop down menu and select **Edit Layout**.
3. **Name**: Enter a unique name for the dashboard.
4. **Description**: Brief description about the dashboard.
5. **No. of Columns**: Select the number of columns that you want to have in the dashboard. By default the number of columns is 2.
6. **Column 1, Column 2, Column 3 & Column 4**: Enter the width of the columns in terms of percentage.
7. Click **Modify** to effect the changes on the dashboard.

Delete Dashboard

To delete a dashboard follow the steps given below:

1. Mouse-over **Dashboards** tab and click on the name of the **Dashboard** that you want to delete. That particular dashboard opens.
2. Now click on **Actions** menu and select **Delete**. A confirmation window pops-up.
3. Click **OK** to confirm deleting.

Note: Default dashboard cannot be deleted.

Managing Different Views

CCTV View

Adding New CCTV

CCTV helps you view only the required dashboards repeatedly at required intervals. To add a new CCTV follow the steps given below:

1. Mouse over **Dashboards** and click **Manage CCTV.**
2. Click **Add CCTV**. Create CCTV window opens.
3. **CCTV Name**: Enter a unique CCTV name.
4. **Description**: Enter a brief description about this CCTV.
5. **Refresh Interval**: Select the interval required to switch over to the next dashboard.
6. Select the desired dashboards that you want to include in this CCTV.
7. Click **Save**.

A new CCTV has been added.

Viewing CCTV

To view a CCTV, mouse-over the **Dashboards** tab and click on the name of the CCTV that you want to view. That particular CCTV opens in a new window.

Editing a CCTV

To edit a CCTV follow the steps given below:

1. Mouse over **Dashboards** and click **Manage CCTV.**
2. Click the edit icon that is corresponding to the name of the CCTV that you want to edit.
3. Make the necessary changes.
4. Click **Save** to effect the changes.

Deleting a CCTV

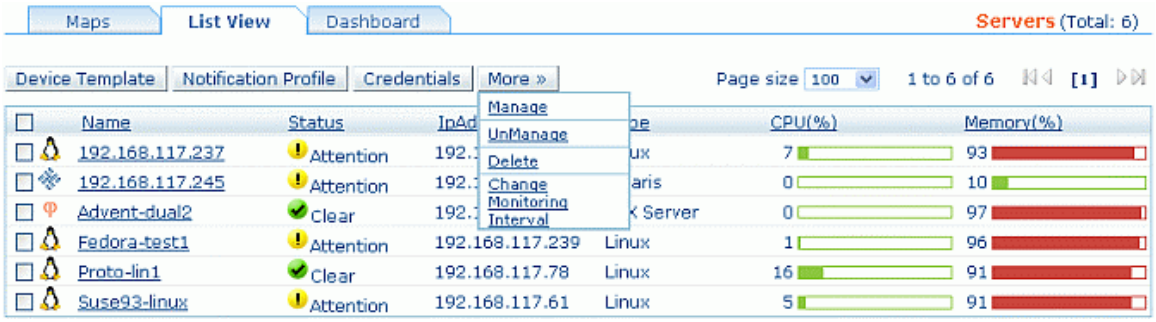
To delete a CCTV follow the steps given below:

1. Mouse over **Dashboards** and click **Manage CCTV.**
2. Click the trashcan icon that is corresponding to the name of the CCTV that you want to delete.
3. A confirmation window pops up.
4. Click **OK** to confirm deleting the CCTV.

The CCTV is deleted.

List View

The List view (Maps-> <Device Category>-> List View) lists all the devices of a category along with their Status, IP Address, Type, % of CPU utilized and % of memory utilized in order to have a quick look at the current status and workload handled by the devices.



The following actions can also be done from here:

- Applying a Device Template
- Associating Notification Profiles
- Applying Credentials
- Managing/Unmanaging Devices
- Deleting Devices
- Changing the monitoring interval of the devices

Applying a Device Template

To apply a device template to the device templates, follow these steps:

1. Select the devices for which you want to apply the template.
2. Click on **Device Template** button.
3. Select the Device Template which you want to apply to the devices.
4. Click **Apply**.

The selected device template is applied to the selected devices.

Associating a Notification Profile

1. Select the devices.
2. Click on **Notification Profile** button.
3. Select the profile to be associated to the devices and click **Next**.
4. Select the fault criteria for the selected profile and click **Next**.
5. Select one of the following options to select the time-window:
    - Apply this profile all the time- This notifies alerts occurring for the selected criteria at any time.
    - Apply the profile for the selected time window- You can specify the required time-window here. For instance, if you set the values as From 09:30 To 18:30, and select the days from Monday through Friday, alerts triggered during the specified interval and selected days only will be notified.
6. Click **Associate** button.

The notification profile gets associated to the selected devices. Note: The notification profiles that are already associated with the devices are left unchanged.

Applying Credentials

1. Select the devices to which you wan to apply the credentials.
2. Click on **Credential** button.
3. Select the credential that you want to get applied to the selected devices.
4. Click **Save**.

The selected credential gets applied to the selected devices.

Managing and Unmanaging devices

1. Select the devices that you want to move to managed or unmanaged state.
2. Click on **More** button and click **Manage/Unmanage**.

The selected devices gets changed to managed or unmanaged state accordingly.

Deleting devices

1. Select the devices that you want to delete or remove from OpManger.
2. Click on **More** button and click **Delete**.
3. A confirmation window pops-up.
4. Click **OK** to confirm deleting.

The selected devices are removed from OpManager.

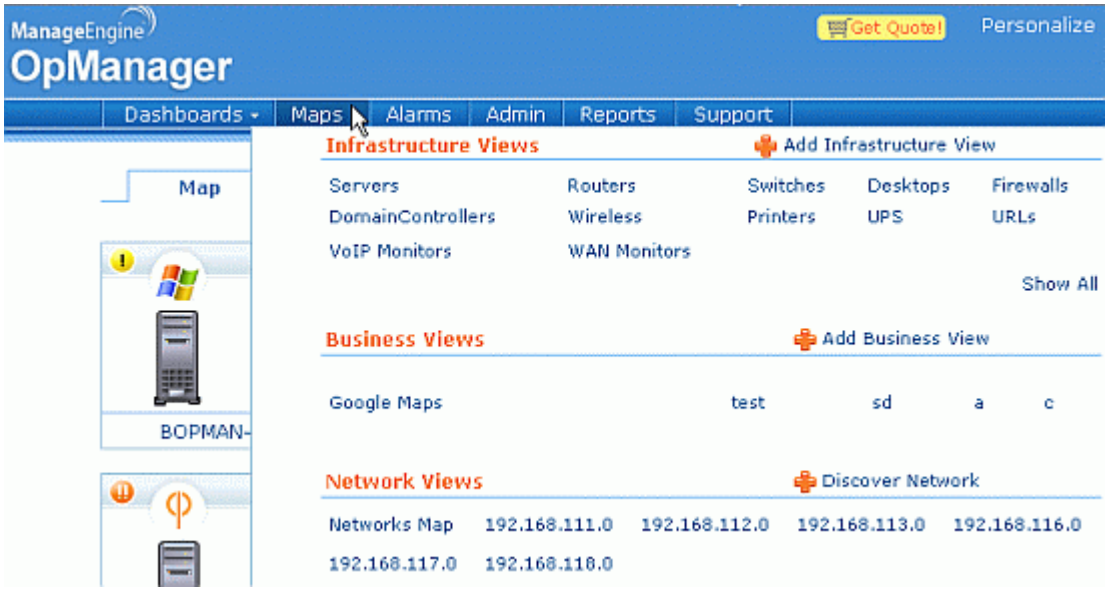
Changing the Monitoring Interval

1. Select the devices whose monitoring interval has to be changed.
2. Click on **More** button and click **Change Monitoring Interval**.
3. Enter the required monitoring interval in terms of minutes.
4. Click **OK**.

The monitoring interval of the selected devices is changed.

Infrastructure Views

Mouse-over Maps tab to access Infrastructure views.



The various category of devices such Servers, Routers, Firewalls etc. monitored by OpManager are listed under Infrastructure Views.Clicking on the Category name, opens the Map View of that category. OpManager also provides you the option to create you own infrastructure view.

Google Maps

OpManager allows you to integrate Google Maps and place the devices on the maps according to the geographic distribution.

Here are the steps to integrate Google Maps and Place devices on them.

- **Providing the Google Maps API Key**

    1. Make sure you have a Google Account or create one.
    2. Mouse-over the Maps tab in the OpManager WebClient.
    3. Click on **Google Maps** link in the Business Views column.
    4. You will be prompted to enter the key. Click on the link **Sign up for a Google Maps API key** to generate a key. You will be taken to a sign up page.
    5. Scroll down the page and provide the website URL as http://<host name running OpManager>. For instance, if the name of the device running OpManager is OpM-Server, your URL will be http://OpM-Server.
    6. Click on the **Generate API Key** button. A key is generated.
    7. Copy the entire Key.

- **Viewing the Google Map in OpManager WebClient**

    1. Go back to the OpManager Webclient and provided the key in the corresponding field.
    2. Click on **Submit Key**.
    3. The Google Map is shown in the interface.

- **Adding Devices on the Google Map**

    1. Now, zoom in/out the map and double-click on the location where you want to place a discovered device.
    2. A device list box pops up allowing you to select a device to be placed in that location.
    3. Select the device and click on **Add**.
    4. Add the required devices on to the map by double-clicking the location.
    5. You can also add the devices to the map from the device snapshot page.
    6. Go to the device snapshot page.
    7. Click on **Add to Google Map** link in the page to add the device to the map.

- **Viewing Device Details from Google Map**

    1. Click on the device balloons on the Google Map to see a popup.
    2. Click the device name/ip address on this popup to get into the device snapshot page.
    3. The popup also shows the device status.

- **Deleting Devices from Google Map**

    1. Click on the device balloons on the Google Map to see a popup.
    2. Click the **Delete** link on this popup to delete the device from the map.

Business Views

OpManager (from build 7000 onwards) comes with an in-built flash-based MapMaker. No more hassles of invoking a separate tool to create business views.

Click the small down arrow in the Maps tab or simply mouse-over. The default maps, with options to add more maps are seen.

Adding Views:

1. From the pop-up in the Maps tab, click Add Business View option.
2. Configure a name for the business view.
3. From the available devices list, select the devices you want to be grouped in this business view, and move them to the right- to the Selected Devices column,
4. Select the background from the corresponding list box.
5. Click Apply.
6. Drop the devices on the map and click on the confirmation check-box that appears.
7. Once the devices are dropped on the map, select and drag-drop the devices to be placed in the required location on the map.
8. Click **Save** button on the left to create and save the map.
9. Click **Exit** to see the newly created business view. You will also find the availability dashboard for the devices in the business view.

Drawing a Link Between Devices

To represent the network diagram in the map, OpManager allows you to draw links between the devices in a business view. You can assign a meaningful name to the link and also configure to change the color of the link to indicate its status.
To draw a link, follow the steps given below:

1. Click the **Add Link** button on the left.
2. From the map on the right, click the device from which you want to draw a link (the source device) and move the mouse to the destination device and click that device. A link properties dialog pops up.
3. Configure a display name for the link.
4. In the **Get Status from** field, select any interface from either the source device or the destination device. The link will inherit the status of the interface that you choose here. For instance, if the source device goes down, and if you have selected an interface from that device, the link also inherits the status of that device.
5. Select the thickness of the link.
6. Click **Apply**.
7. Click **Save** on the left to save the changes.

Modifying Business Views

You can make changes to the business views created. Access the business view either from the Maps tab or from the list of views under the Home tab. Click the Edit icon to modify the view properties. After you modify the properties like adding/removing links, adding more devices to the view, adding shortcuts on the view, changing background etc, click the **Save** button on the left to save the changes.

Adding Shortcuts

You can add shortcut icons to business views that helps you to drill-down the network. This helps you to easily navigate to a view from another view when objects are grouped based on their geographical location.

Note: You must have created atleast two business views to be able to add a shortcut from one view to another.

Here are the steps to add shortcuts on the business views:

1. Go the the business view and click the Edit option on right-top corner of the view.
2. Click the Add Shortcut button on the left. A shortcut properties dialog pops up.
3. Configure a name for the shortcut in the **Shortcut Name** field.
4. From the **Open Submap** list-box, select the map which should be opened when you click the shortcut.
5. Select the icon to be used for the shortcut from the **Default Icons** or select from the **Custom Icon** combo-box.
6. Click Apply for the shortcut to be added.

Network Views

Mouse-over Maps tab to access the network views. The various networks that are discovered and monitored by OpManager are listed under Network Views. Clicking on the network's IP address opens the Map view of that network. Clicking on Network Map link displays the layout of that network's LAN connection.

Alerting

Managing Faults in Network

There can various types of faults in a network. With the network health depending on various resources like the system resources, services, network connectivity etc, getting to the root of the problem is simplified when the monitoring solution raises meaningful alarms. OpManager helps you identify the fault quickly with its detailed alarms indicating the resource that is poorly performing in the device . The different types of OpManager alarms include:

- Status-poll Alarms (device, service, interface, port down alarms).
- Threshold-based alarms for host resources, response times etc proactive monitoring.
- Alarms from SNMP Traps.
- Windows event logs based alarms.

OpManager monitors the resources for availability and performance and triggers alarms for all the criteria mentioned above. These alarms can also be sent as email or sms alerts from OpManager.

Viewing Alerts

The Alarms tab in OpManager shows all the latest alerts.

From the list box on the top right corner, you can access the following:

- **All Alarms**: A complete list of alarms is displayed here.
- **Active Alarms**: This view lists only the active alarms that are not yet cleared
- **Unsolicited Traps**: The unsolicited traps sent by the agents in the managed devices are listed here. These are the traps that are not configured to be processed in OpManager. If you find any of these traps to be critical, you can configure OpManager to process the traps using the information received from the agent. Refer to Creating a Trap Processor for details.
- **Windows Events**: This view lists only the alarms that are triggered from Windows event logs as the source.
- **Devices to Watch**: You can view the devices with fault in this list view.

Alert Actions

You can perform the following alert actions:

Acknowledge: This option is useful for the operators to pick up the problem and work on it. When you select an alarm and click on Acknowledge button on top the alarms list, the administrator/operator's name is populated in the technician's field. Note: Alarms that are acknowledged can be excluded from being escalated by configuring accordingly the alarm escalation rule.

Unacknowledge: The assigned technician is removed and the alarm is back in the unassigned list.

Clear: You can click this to clear an alarm manually.

Delete: You can delete an alarm.

View History: Click on the alarm message to view the alarm details and event history.

Adding Notes:You can add notes to the alarms to explain the steps you have followed to correct the fault or to give tips to the operator who is working on the fault. In the Alarm history page, click the **Add Notes** option.

Escalating Alarms

The alarms of critical devices should not be left unnoticed for a long time. For instance, the mail-servers, web-servers, backup-servers, switches, and routers are so critical that if their faults are not solved within a specified time, the networking functionality will be brought down. You can configure OpManager to escalate such unnoticed alarms by sending an e-mail to the person concerned. However, you have an option to exclude the alarms that are acknowledged from being escalated.

To configure a new alarm escalation rule, follow the steps given below:

1. Click the **Admin** Tab.
2. Under **Alerts**, click **Alarm Escalation**.
3. Click **Add Rule** to create a rule.
4. Assign a name to the rule in the **Rule Name** field.
5. Select the **Severity** and **Category** of the alarm.
6. Select the **Business View** in order to associate the rule only to the alarms of the devices of the selected business view. If not select None to associate the rule to the alarms of all the devices.
7. Then configure the the interval in either hours or minutes to wait for the alarm to get cleared.
8. You can exclude the acknowledged alarms from being escalated by selecting **Exclude Acknowledged Alarms** option.
9. Type the values for the fields under **Escalation Email Details** to send an e-mail if the alarm is not cleared within the specified interval.
10. Configure the **From Email Address**, the **Subject** and the **Message** of the escalation mail.
11. In the **Run this check every** box, set the interval in minutes to execute this rule.
12. Click **Save**.

If you configure a new alarm escalation rule, by default it will be enabled. To disable an alarm escalation rule click on Edit icon, deselect the **Enable this rule** option and click on **Save**.

Receiving SNMP Traps in OpManager

OpManager listens for SNMP traps from devices on the default port 162. So, it automatically acts as a trap receiver and based on the trap processors defined in OpManager, the traps are processed and shown as OpManager alarms.

Processing SNMP Traps into Alarms

OpManager enables you to process the traps from the managed devices. When a trap is received from a managed device, OpManager notifies the administrator with an alarm. You can configure the severity and the message of the alarm generated for the traps. Some of the common traps are automatically processed in OpManager into alarms. You can see all these trap processing configuration from Admin --> SNMP Trap Processors.

The devices must be SNMP-enabled so that it can send traps to OpManager when there is a problem. You can configure more trap processors in OpManager for other type of traps.

Different Trap Types

Trap Name	Trap Description	Severity
LinkUp	A communication interface has been enabled.	Clear
LinkDown	A communication interface has been disabled.	Critical
AuthenticationFailure	A message that cannot be authenticated has been received.	Trouble
EgpNeighborLoss	An Exterior Gateway Protocol (EGP) neighbor has been lost.	Trouble
ColdStart	The agent is reinitializing. The SNMP data and configuration might have changed.	
WarmStart	The agent is reinitializing without any change in the SNMP data and configuration.	Attention
Cisco Voltage Change Status	The voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the Cisco Shutdown trap.	Trouble
Cisco Config Management Event	The Cisco configuration has been changed.	Trouble
Cisco Temperature Change Status	The temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the Cisco Shutdown trap	Trouble
Redundant Supply Notification	The redundant power supply (where extant) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the Cisco Shutdown trap.	Trouble
Cisco Fan Status	One of the fans in the fan array (where extant) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the Cisco Shutdown trap.	Trouble
Cisco Shutdown	The environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown. This notification contains no objects so that it may be encoded and sent in the shortest amount of time possible. Even so, management applications should not rely on receiving such a notification as it may not be sent before the shutdown completes.	Critical

Loading Traps from other MIBs

Following are the steps to load the traps from various MIBs.

1. Under the **Admin** tab, select **SNMP Trap Processors**. All the configured processors are listed here.
2. On the right, select **Load From Mibs** under **Actions**
3. From the list of MIBs, select the MIB from which you would like to load the trap variable. The traps in that MIB are listed.
4. Select the required trap variable, and click **Add Trap Processor(s)**.

A Processor for the selected trap is added, and is listed under the SNMP Trap Processors.

Adding New Processors Directly

You can add processors for traps from any custom SNMP MIB. OpManager can extract useful information that is sent with SNMP traps as variable bindings (SNMP varbinds). So if you have bought devices from different vendors, all you need to do is get access to those vendor-specific MIBs and you can easily have OpManager monitor critical variables on that device.
If a managed device sends a trap that has not been defined, you can view them in the Unsolicited Traps view until a processor is configured.

To create a trap processor, follow the steps given below:

1. Click **SNMP Trap Processors** under the **Admin** Tab.
2. Click **Add Custom** under **Actions**.
3. Fill in the values for the text fields in this dialog.
4. Click **Add**.

The processor is added.

Configuring Notifications

When a fault is detected in your network, an event occurs and multiple events correlate to trigger an alarm. You can configure OpManager to notify the network administrator or perform automatic actions based on the alarm raised for a device.

The different types of notifications available are:

- Email Alerts
- SMS Alerts
- Web Alerts
- Run a Program
- Run a System Command
- Log a Ticket (Trouble ticketing in ServiceDesk Plus)

The configured notification settings are available as profiles and these can be associated to different devices for different fault criteria.

Configuring Mail Server Settings

OpManager allows you to configure e-mail alerts and SMS alerts to get notified on the fault in your network. By default, OpManager sends the mail to the mail server specified in the e-mail notification profile. To configure the SMTP server settings globally and to provide the secondary mail server settings, follow the steps given below:

1. Under the **Admin** tab, click **Mail Server Settings**.
2. Enter the SMTP **Server name** and **Port** number.
3. Select **Requires Authentication** and enter the **User name** and **Password** details, if the server requires authentication to send e-mail.
4. Configure the **From** and **To Email ID** fields.

Verifying Configuration

- To test the settings enter the **Email ID** and click **Test Mail**. This e-mail ID will be considered as the default To Email ID while creating Email and SMS notification profiles.
- If you have a secondary mail server in your network, select **Add a secondary mail server** and provide the details. In case of failure of primary mail server, OpManager uses secondary mail server to send e-mail and SMS.

Configuring Proxy Server Settings

Any business enterprise will have a proxy server to optimize its connectivity to Internet and to filter access to restricted Web sites. In OpManager, to monitor URLs over internet, you need to provide the proxy server details of your enterprise.

To enter the details, follow the steps given below:

1. Under the **Admin** tab, click **Proxy Server Settings**.
2. Select the **Enable Proxy** check-box.
3. Enter the Proxy server name, port number in which the Web service is running on the proxy server, and the user name and password to connect to the proxy server.
4. For the devices that do no require to go through a proxy, specify the name or the IP Address of the devices as a comma separated list in the **No Proxy** field.
5. Click **Save** to save the details.

Configuring SMS Server Settings

Besides the email-based SMS notifications, OpManager allows you to configure modem-based SMS alerts. Configure the SMS Server Settings in OpManager as follows:

1. Ensure if yours is one of the supported modems.
2. Connect the GSM Modem to the Serial Communication Port.
3. Go to Admin --> SMS Server Settings.
4. Configure the port number to which the Modem is connected.
5. Click OK.

Configuring Email Alerts

You can configure OpManager to send e-mail to network administrators when a fault is detected in the device. You can create separate profiles for each administrator and assign them to devices so that whenever the device has a fault, an e-mail is sent to the technician concerned.

To create an email alert profile, follow the steps given below:

1. Select Admin --> Notification Profiles
2. Click **Add New** option against **Email Alerts**.
3. Type the profile name.
4. Type valid **To** and **From** Email addresses.
5. Select the required alarm variables that you would like to see in the email alert.
6. Click Associate link on the right to associate the profile to devices.
7. Select the Profile and click **Next**.
8. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Click Next
9. Select the devices or the category of devices for which you want to be notified. For instance, if you want to be notified of threshold violation for all Servers, select Server category from the combo-box. Click Next.

The profile is associated to all the servers. A notification is sent every time a threshold is violated for a server.

Note: Primary and secondary SMTP server settings can be provided in the Mail Server Settings page in OpManager. Whenever a new email profile is created, the values of the primary SMTP server and the authentication details are retrieved from the Mail Server settings. Refer to Configuring Mail Server Settings for steps to enter the details. If the SMTP server is not available while sending e-mail, secondary mail server is used to send the mail automatically.

Configuring SMS Alerts

You can configure OpManager to send SMS to network administrators whenever a fault is detected in the device. You can create separate profiles for each administrator and assign them to devices so that whenever a device has trouble, depending on the trouble, SMS is sent to the technician concerned.

OpManager supports email-based SMS alerts and also modem-based SMS alerts.

Please note that Modem-based SMS alerts comes as an add-on over OpManager and needs to be licensed seperately.

Modem-based SMS Alerts

To create a modem-based SMS notification profile, here are the steps:

1. Configure the SMS Server Settings.
2. Click the **Admin** tab.
3. Under **Alerts**, click **Notification Profiles**.
4. From **Modem-based SMS** column, click **Add New**.
5. Type the profile name.
6. Type the mobile number.
7. Select the required alarm variables. The selected variables will be seen in the sms alert received.

Refer to the support modems list to use this notification profile.

Email-based SMS Alerts

To create an email-based SMS notification profile, follow the steps given below:

1. Configure the Mail Server Settings if you have'nt configured yet.
2. Click the **Admin** tab.
3. Under **Alerts**, click **Notification Profiles**.
4. From **Email-based SMS** column, click **Add New**.
5. Assign a meaningful name to this profile.
6. Type valid To and From Email addresses.
7. Select the required alarm variables that you would like to see in the sms alert.
8. Save the Profile.
9. Associate the profile to the required devices. This triggers alerts when faults occur.

Note: Primary and secondary SMTP server settings can be provided in the Mail Server Settings page in OpManager. Whenever a new SMS profile is created, the values of the primary SMTP server and the authentication details will be considered from the Mail Server settings. Refer to Configuring Mail Server Settings for steps to enter the details. If the SMTP server is not available while sending e-mail, secondary mail server will be used to send the mail automatically.

Configuring Web Alarm Notifications

Configure OpManager to notify you by way of a web alarm when there is a specific fault.

Here are the steps to configure a Web Alarm Notification Profile:

1. Go to Admin > Notification Profiles > Web Alarm
2. Click **Add New** against the Web Alarm profile.
3. Configure the following values to create the profile:
    - **Profile Name**: Configure a name for the notification profile.
    - **Select Users**: Select the users for whom Web Alarms should be enabled.
    - **Test Actions**: Click this button to confirm if the Web Alarm sound is produced.
4. Click **Save** to create the profile.

You will hear the alarm sound when logged-in as any of the selected users.

Note: The Web Alarms are available only for the user sessions selected above.

Using a Run Program Notification Profile

You can configure OpManager to automatically run a program whenever a fault is detected in the device. For instance, you can configure OpManager to execute a program that corrects the fault or simply produces a sound or that whenever a specific type of an alarm is raised for a device.

To create a profile that executes the specified program, follow the steps given below:

1. Select Admin --> Notification Profiles
2. Click **Add New** option against **Run Program**.
3. Type the profile name.
4. In the **Command Name** field, specify the name of the program to be executed with the absolute path. Example C:\profiles\testprogram.bat.
5. If the program requires some arguments, specify the arguments.
6. Save the profile.
7. Click Associate link on the right to associate the profile to devices.
8. Select the Profile and click Next.
9. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Click Next
10. Select the devices or the category of devices for which you want to be notified. Click Next.

The profile is associated to all the servers. The program is executed with the specified arguments whenever a fault matching the selected criteria occurs.

Using a Run Command Notification Profile

You can configure OpManager to automatically run a system command whenever a fault is detected in the device. For instance, you can configure OpManager to execute a netsend command to send popup messages to users machines whenever a specific type of an alarm is raised for a device.

To create a profile that executes the specified program, follow the steps given below :

1. Select Admin --> Notification Profiles
2. Click **Add New** option against **Run System Command**.
3. Type the profile name.
4. In the **Command String** field, specify the command name with additional arguments if any.
5. Select the **Err Append** and **Append** check-boxes to append the output and the error message on executing the command.
6. Save the profile.
7. Associate the profile to devices.

The system command is executed with the specified arguments whenever a fault matching the selected criteria occurs.

Creating a Sound Notification Profile

By default, OpManager provides a sound notification that plays a beep sound when a fault is detected in the associated devices. You can also create profiles to play the sound of your interest.

To create a sound profile, follow the steps given below:

1. Copy the sound file you want to play in the *<OpManager Home>/conf/application/scripts* directory.
2. Create a Run Program notification profile with the following values to the fields:

   Command Name: ./jre1.4.1/bin/java
   Program arguments: -classpath ./classes/OpManagerServerClasses.jar com.adventnet.me.opmanager.server.alert.AudioNotifier ./conf/application/scripts/<audio_file_name>

You need to associate the profile to the device for triggering it during a fault. The sound can be heard in the OpManager server.
.

Modifying and Deleting Notification Profiles

You can modify or remove an existing notification profile. Here are the steps:

1. From the Admin tab, select **Notification Profiles**.
2. All the configured profiles are listed here.
3. Click the **Delete** icon against the profiles name to delete the profiles.
4. Click the **Edit** icon against the profiles name to modify the profile properties.

The changes made here are applied for all the devices to which the profile is associated.

Associating Notification with Managed Devices

You need to associate the notification profiles with devices to trigger the corresponding action whenever these devices are under trouble. You can also select the time-window so that alerts during the specified interval only is notified.

To associate a profile with devices or a category of devices, you can use the Quick Configuration wizard. For doing so, follow the steps given below:

1. From the **Admin** tab, under **Configuration**, click **Quick Configuration wizard**.
2. Select **Assign a notification profile...** and click **Next**.
3. Select the profile to be associated to the devices and click **Next**.
4. Select the fault criteria for the selected profile and click **Next**.
5. Select one of the following options to select the time-window:
    - Apply this profile all the time- This notifies alerts occurring for the selected criteria at any time.
    - Apply the profile for the selected time window- You can specify the required time-window here. For instance, if you set the values as From 09:30 To 18:30, and select the days from Monday through Friday, alerts triggered during the specified interval and selected days only will be notified.
6. Select one of these options to associate the profile and click **Next**.
    - If you select a category, then the profile is associated to all the devices in the category automatically.
    - If you choose Select devices manually, the next page will list all the managed devices. Move the devices from the list in the left to the one in the right and click **Finish**.
    - If you select a business view, the profile is associated to all the devices in the selected view.

To associate a notification profile to a single device, follow the steps given below:

1. Open the snapshot page of the device.
2. Select the **Notification Profiles** tab at the bottom.
3. Click the corresponding link to select and associate the required profiles.

Add-ons & Plug-ins

VoIP Monitor

About VoIP Monitor

Cisco IPSLA monitor or VoIP monitor comes as an add-on feature in OpManager and requires licenese to run. OpManager continuously monitors the key performance metrics of the VoIP network to determine its health. The parameters measured include Jitter, Latency, Packet Loss etc.

Jitter: Jitter indicates a variation in delay between arriving packets (inter-packet delay variance). Users often experience uneven gaps in speech pattern of the person talking on the other end, and sometimes there are disturbing sounds over a conversation coupled with loss of synchronization etc.

Latency: The delay measured is the time taken for a caller's voice at the source site to reach the other caller at the destination site is called as latency. Network latency contributes to delay in voice transmission, resulting in huge gaps between the conversation and interruptions.

Packet Loss : Packet loss is a measure of the data lost during transmission from one resource to another in a network. Packets are discarded often due to network latency.

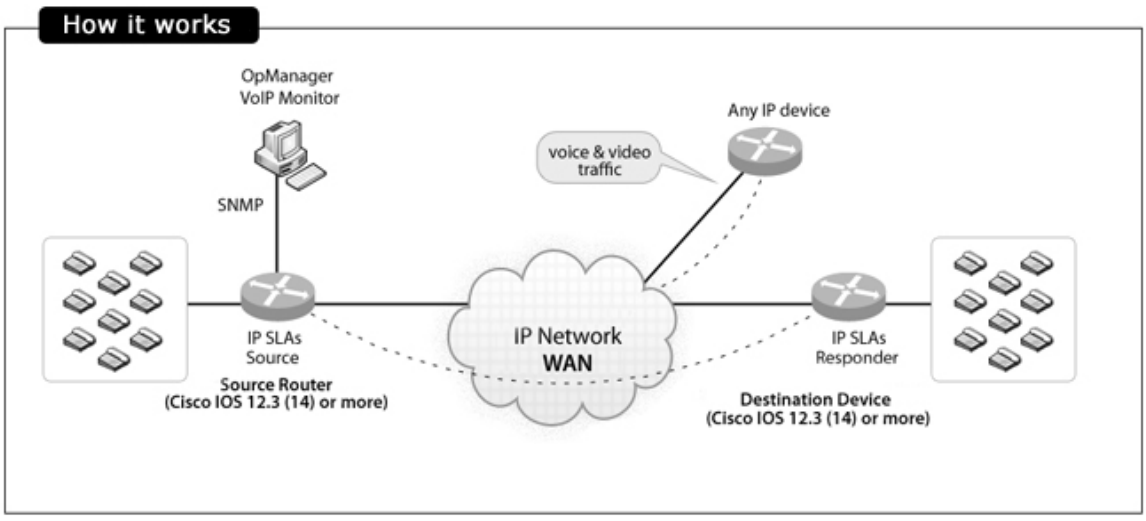
MOS: The jitter codec determines the quality of VoIP traffic and each codec provides a certain quality of speech. The Mean Opinion Score is a standard for measuring voice codecs and is measured in the scale of 1 to 5 (poor quality to perfect quality). The quality of transmitted speech is a subjective response of the listener.

How it works

OpManager primarily relies on Cisco's IP-SLA for monitoring the VoIP and the prerequisite therefore is, that the device should be a Cisco Router and must have IPSLA agent enabled on it. From IOS Version 12.3(14)T all Cisco routers support monitoring of VoIP QoS metrics.

Cisco's IPSLA, an active monitoring feature of Cisco IOS software, facilitates simulating and measuring the above mentioned parameters to ensure that your SLAs are met.

Cisco IP SLA provides a UDP jitter operation where UDP packets are sent from the source device to a destination device. This simulated traffic is used to determine the jitter, the round-trip-time, packet loss and latency. This data is gathered for multiple tests over a specified period to identify how the network performs at different times in a day or over a few days. The VoIP monitor gathers useful data that helps determine the performance of your VoIP network, equipping you with the required information to perform network performance assessment, troubleshooting, and continuous health monitoring.



Adding a New VoIP Monitor

Prerequisites

When you want to test a link from your office to another location, you need a Cisco router (IOS version 12.4 or later) at each end.

Steps to set up the monitor

Using OpManager, you can now monitor the voice and video quality of a 'call path'. Call path is the WAN link between the router in your main office and the one in the branch office that you want to monitor.

Step 1 : Enable Add (/discover) the router in your LAN to OpManager. And make sure the SNMP read and write community are configured properly, for that router.

Step 2: Enable SLA responder on the destination device you wish to monitor, Steps are detailed below.

a. Open a CLI session on the destination router and enable the EXEC mode as follows:

   Router>enable

b. Start the global configuration mode:

   Router#configure terminal

c. Enable the IP SLA responder:

   Router(config)#ip sla responder
   [or]
   Router(config)#ip sla monitor responder
   (Note: Enter any one of the command to enable IP SLA responder as it varies according to the IOS versions.)

d. Repeat the above steps for all the destination routers on which you want to monitor VoIP performance.

Step 3: Creating the VoIP monitor:

a. Go to Home-> VoIP Monitors->Configure VoIP Monitor-> Create New, and enter a name for the monitor.
b. Select the source router from the list of routers discovered in OpManager, and select the relevant interface.
c. Specify the destination router either by using the 'Search' option to pick from the discovered routers, or use the 'Add' option to specify the IP address of the destination router and submit the details.
d. You will see the summary of the monitor you are about to configure. Now click 'Apply to device' to submit the details to the device. This will take few seconds to configure.
   Refresh the page after few seconds to see the new monitor. The data will be collected every hour, from the time you have configured.

[or]

You can also create the VoIP monitor from the Router snapshot page. To do so, go to Router snapshot page, click on Action tab and select Add VoIP Monitor. Enter the Monitor Name and Destination IP. Click Submit to create the monitor or Click Advanced button to go to Create New VoIP Monitor page and follow the steps from b to d given under Step 3.

To edit any of the configuration details, go to the respective template, make the changes and save the details. When you create a new monitor, the updated values take effect. When the configuration is complete, the router starts collecting the data at the specified frequency 60 seconds (default value). OpManager updates this statistics (collected data) every hour and the reports are generated after one hour of configuration. Go through the FAQs section to understand QoS parameters.

Configuring call settings and threshold template

Defining Call Settings:

Define a template with the required VoIP settings to be used for monitoring performance. The VoIP template comes with pre-populated default values. Incase you would like to effect some changes to the values before initiating monitoring, make the changes as follows:

1. Mouse-over Maps tab and click VoIP Monitors.
2. Go to Settings-> Call Settings.
3. Configure the following parameters:

Destination Port - Specify the VoIP UDP port to which VoIP Monitor sends simulated traffic to generate performance metrics. The default port number is set as 16384. You can specify a port in the range of 16384 - 32766.

Simulated VoIP Codec - The VoIP jitter codec decides the type of traffic that VoIP Monitor simulates over your network.

Operation Frequency - The operation frequency is the frequency with which QoS metrics are collected by the IP SLA agent on your network to determine performance.

Operation Timeout - The operation timeout is time to wait for the response from the responder / destination device in msecs.

Type of service - The Type of Service octet allows you to set precedence levels for VoIP traffic of the IP SLA operations.

MOS Advantage Factor - The advantage factor is a measure, on a scale of 0 to 20, of the willingness of your VoIP network users to trade call quality for convenience

Defining Thresholds for the monitored parameters:

You can define a threshold template so that the VoIP performance parameters can be better suit your company SLA's (Service Level Agreements). Alerts are triggered based on the thresholds configured so that you can take corrective actions in time. Here are the steps to define a threshold template:

1. Mouse-over Maps tab and click VoIP Monitors.
2. Go to Settings->Threshold Template.
3. Configure the following values:

MOS Threshold : Configure the MOS threshold by specifying the upper and lower MOS range values in the range of 1 to 5.

Jitter Threshold : Configure the jitter threshold in msecs with upper and lower threshold limits. The range is from 0 to 6000 msecs.

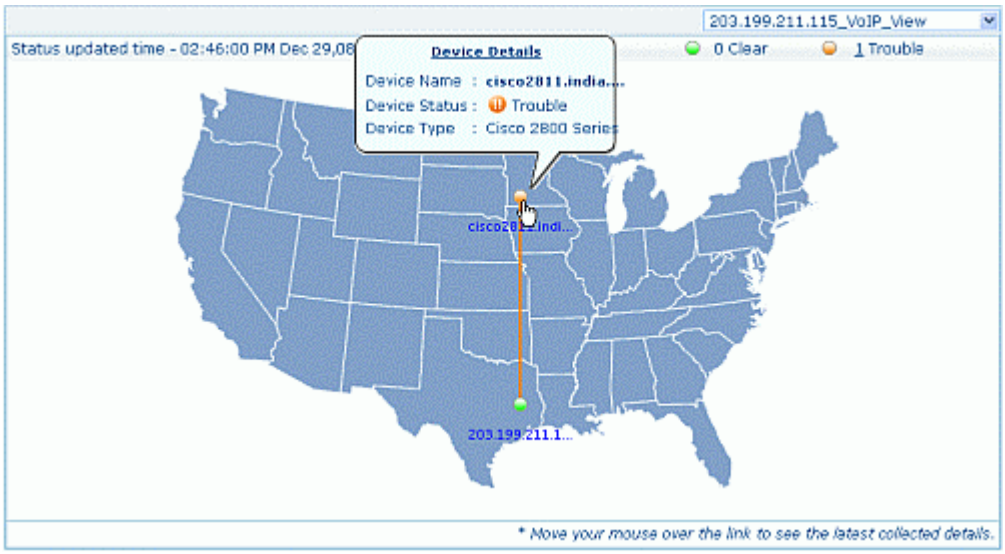
Latency Threshold : Specify the delay allowed in msecs again in the range of 0 to 6000.

Packet Loss : Specify the number of packets that can be lost in transit.

Notification Profile : Select the required notification profile(s) in order to notify when the any threshold rule is violated.

Business Views in VoIP Monitor

In VoIP Monitor, business views help you to know the status of the device and call path between devices at a glance. Whenever a new VoIP monitor is created, a business view (image shown below) of it also gets created automatically with the default background and device icons. However, later you can modify the background and device icons if required.



In the business view, mouse-over the device icon or name/IP and call path to view its details. Click on the device icon or call path will open the snapshot page of the device or the call path respectively.

Accessing VoIP Monitor Business Views

1. Mouse-over **Maps** tab and select **VoIP Monitors**.
2. Click **Business Views**.
3. Select the required business view from the drop down menu available on the top the business view displayed.

Viewing Top 10 Call Paths

With VoIP Monitor you can view the top 10 call paths by MOS, Packet Loss, Jitter and Latency. This provides you to have a quick view and react proactively. To view the top 10 call paths, follow the steps given below:

1. Mouse-over **Maps** tab and click on **VoIP Monitors**.
2. Click on **Top 10**. The top 10 call paths by MOS, Packet Loss, Jitter and Latency are listed.
3. Click on the required call path view its snapshot page.

Viewing VoIP Monitor Alerts

Go to Maps-> VoIP Monitor-> Alerts to view the alerts raised by WAN Monitor. All the alarms are listed with the Source name, Alarm Message, Status of the Device, Technician, Device category, date and time. Click the alarm message to view the alarm history.

Viewing VoIP Monitor Reports

The VoIP Monitor reports help you to view the various metrics such as jitter, MOS, RTT etc. to determine the health of the VoIP networks. To generate the VoIP monitor reports, follow the steps given below:

1. Mouse-over **Maps** tab and select **VoIP Monitors**.
2. Click on **Reports**. The default **History reports** and **Top N reports** are listed.
3. Click on the required report.

You can also access the VoIP Monitor reports from Reports tab. The generated report can be emailed or exported to a PDF version by click the respective icons on the report.

FAQs on VoIP Monitor

1. Why do i need to set SNMP write community on the Source Router ?

Both, the SNMP read and write community string needs to be set on the source router. The write community is used to configure the IPSLA on the device while the read community is used by OpManager to gather performance data from the router.

2. Why I am getting 'Source router SNMP write community may be wrong' error message?

OpManager uses SNMP to gather data from the Cisco IP SLA agent. This error is displayed when wrong SNMP read / write community string is configured for the Source router of the VoIP Monitor in OpManager.

To configure the correct SNMP write community string in OpManager, go to the snapshot page of the source router and change the SNMP credentials by clicking on the '**Click here to change**' corresponding to the "**Passwords**" field. In the pop-up enter the appropriate credentials and submit it. After successfully submitting the correct SNMP credentials, try to add the VoIP Monitor again for the Source device (Maps > VoIP Monitor > Settings).

3. Why should the SLA Responder be enabled on the destination device ?

Enabling the IP SLAs Responder provides the details of packet loss statistics on the device sending IP SLAs operations. IP SLAs Responder is enabled on the target router (rtr responder) before configuring a Jitter operation.

4. Why are the VoIP metrics shown as zero or 'Not available' in OpManager?

You will see zero or 'not available' values when data is not collected for the monitored metrics. This can be either due to incorrect SNMP read community configured, or of the Responder is not enabled on the destination device. Make sure that the correct SNMP read community is configured and the SLA Responder is enabled.

5.What are the critical parameters monitored to determine the VoIP QoS performance?

The monitored parameters include Latency, Jitter, Packet Loss, and MOS. The parameters are described below for reference:

Jitter : Jitter is defined as a variation in the delay of received packets. Users often experience disturbing sounds over a conversation coupled with loss of synchronization at times and is referred to as jitter. High levels of jitter can result in some packets getting discarded and thereby impact the call quality. Ensuring a jitter-free transmission to provide qualitative service depends on identifying the bottle-neck responsible for the jitter, and acting on it to eliminate it. OpManager's VoIP monitoring feature helps you find the problem and ensures maximum QoS on your VoIP network.

Packet Loss : Packet loss is a measure of the data lost during transmission from one resource to another in a network. Packets are discarded often due to network latency. Using OpManager, you can monitor the packet loss and take corrective actions based on the information.

One way Latency: Latency (delay) is the time taken for a packet to reach the destination device. When monitoring latency over VoIP, the delay measured is the time taken for a caller's voice at the source site to reach the other caller at the destination site. Network latency contributes to delay in voice transmission, resulting in huge gaps between the conversation and interruptions.

Round Trip Time: Round Trip Time is the time taken for a packet to reach the destination and again comes back to the source device. The total time it takes for the round trip is measured in milliseconds.

MOS: The Mean Opinion Score is the key quality indicator of VoIP traffic quality. And is measured in the scale of 1 to 5 (poor to excellent quality).

6. What is VoIP codec?

Codecs (Coder/Decoder) serve to encode voice/video data for transmission across IP networks. The compression capability of a codec facilitates saving network bandwidth and it is therefore appropriate that you choose the correct codec for your IP network. Here is a quick reference to the codecs with the corresponding packets size and bandwidth usage:

Codec & Bit Rate (Kbps)	Operation Frequency	Default number of packets	Voice Payload Size	Bandwidth MP or FRF.12 (Kbps)	Bandwidth w/cRTP MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G.711a/u (64 kbps)	60 msecs by default. You can specify in the range of 0 - 604800 msecs.	1000	160 + 12 RTP bytes	82.8 kbps	67.6	87.2
G.729 (8 kbps)		1000	20 + 12 RTP bytes	26.8 kbps	11.6	31.2

7. How much bandwidth does each monitor occupy ?

The bandwidth occupied depends on the codec selected. Look at the above table for reference.

WAN Monitor

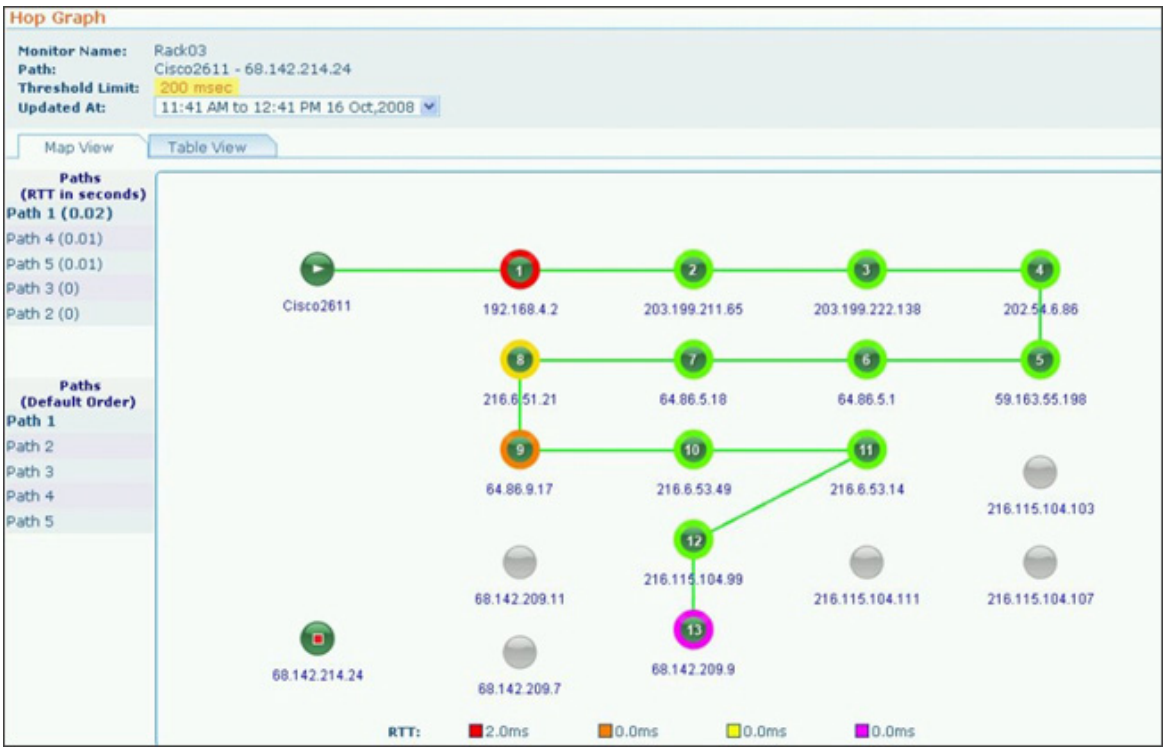
About WAN Monitor

The WAN monitoring feature in OpManager is an add-on feature and requires license to run. The WAN monitor monitors the availability of all your WAN links, the Round Trip Time (RT) / Latency and the traffic details. Alerts are triggered when the set thresholds are violated, enabling the administrators to attend to the fault in no time.

OpManager uses Cisco's IPSLA agent to monitor the health and performance of the WAN links, and the prerequisite therefore is, that the device must be a Cisco router (IOS version 12.3 or later) and it should have IPSLA agent enabled on it . Almost all the routers from Cisco are enabled with IPSLA agent and we support from IOS version 12.3 or later. The performance of the WAN link is measured by sending simulated traffic (packets of specified size) at a specified frequency. So the health of the WAN link / path is monitored round the clock . It helps the IT Engineer to proactively notice the problem. The Round Trip Time data is collected and persisted to measure the performance and also for reporting. Also, OpManager triggers alert when a Round Trip Time threshold is violated.

OpManager collects IPSLA traps for events triggered due to a connection loss or threshold violation for RT. When any such failure occurs, OpManager immediately triggers a Trace Route operation automatically to help the IT Engineer trace the fault to the exact hop. Further, the Trace Route report shows RT data for five different paths and 15 hops in a path. This enables you to troubleshoot and get to the root of the problem much quicker, resulting in very less downtime.

Besides this intelligent monitoring of the links across each hop, Netflow traffic reports also integrated in this new release. This enables you to identify any latency caused by the LAN traffic. You simply need to select all the WAN links / path to be monitored once and configure it. A sample trace route graph is given below:



Configuring WAN Monitor

Prerequisites

OpManager primarily relies on Cisco's IP-SLA for monitoring the WAN and the prerequisite therefore is that the device should be a Cisco router and must have IPSLA agent enabled on it. Almost all the routers from Cisco were enabled with IPSLA agent and we support from IOS version 12.3 or later. OpManager uses SNMP to query the Cisco routers for the links' performance data. IPSLA familiarity is not a prerequisite. You just need to tell OpManager which links you want to monitor. OpManager provides an intuitive configuration wizard to help you configure all the IPSLA parameters for monitoring the WAN health.

Steps to set up the WAN Monitor

Using OpManager, you can now monitor the availability and latency of a WAN link / path. A WAN link mentioned here is the path between the router in your main office and the one in the branch office that you wish to monitor.

Step 1 : Add (/ discover) the router in your LAN to OpManager. And make sure the snmp read and write community are configured properly, for that router.

Step 2: Configuring the Router to send traps

Configure the cisco router to send traps to OpManager. Alerts are shown based on the traps received in OpManager. To configure OpManager server as the SNMP Server receiving traps for the routers, telnet the router and type the following command:

snmp-server host <opmanager server IP> traps <host community string> rtr

For instance, if the OpManager host IP Address is 192.168.18.128, and the community string is private, the command would be:

snmp-server host 192.168.18.128 traps private rtr

Step 3: Creating the WAN Monitor

a. Go to the Maps tab (on from the list of Infrastructure views), click on-> WAN Monitors-> Settings
b. Select the source router from the list of routers discovered in OpManager and then select the relevant interface of the source router
c. Specify the destination Ip Address either by using the 'Search' option to pick from the discovered routers, or directly enter the IP Address and click 'Add' and submit the details.
d. You will see the summary of the monitor you are about to configure. Now click 'Apply to device' to submit the details to the device. This will take few seconds to configure. Refresh the page after few seconds to see the new monitor. The data is collected every hour, from the time you have configured.

[or]

You can also create the WAN monitor from the Router snapshot page. To do so, go to Router snapshot page, click on Action tab and select Add WAN Monitor. Enter the Monitor Name and Destination IP. Click Submit to create the monitor or Click Advanced button to go to Create New WAN Monitor page and follow the steps from b to d given under Step 3.

To edit any of the configuration details, go to the respective template, make the changes and save the details. When you create a new monitor, the updated values take effect. When the configuration is complete, the router starts collecting the data at the specified frequency 60 seconds (default value). OpManager updates this statistics (collected data) every hour and the reports are generated after one hour of configuration.

Configuring Test Parameters and Threshold Template for WAN Monitor

Define a template with the required WAN monitoring settings to be used for monitoring performance. The RTT template comes with pre-populated default values. OpManager uses the configured values to simulate traffic. Incase you would like to effect some changes to the values before initiating monitoring, make the changes as follows

Configuring Test Parameters

OpManager uses the default settings specified here,

- **Payload**:The default value is 24 kb. Specify an echo payload value in the range of 0 to 16384.
- **Type of Service**: Specify the Echo TOS in the range of 0 to 255, the default being 30.
- **Operation Frequency**: Specify the interval in the range of 0 to 604800 msecs. The default interval is 60. The operation frequency is the frequency with which QoS metrics are collected by the IP SLA agent on your network to determine performance.
- **Operation Timeout**: Specify the timeout in the range of 0 to 604800000, the default being 60 msecs. Make sure that the timeout interval is lesser than the configured operation frequency so that if the operation is not successful, that is, if there is no response from the device, or in the event of a delay, the request is timed out and the subsequent operation is launched at the configured frequency correctly.

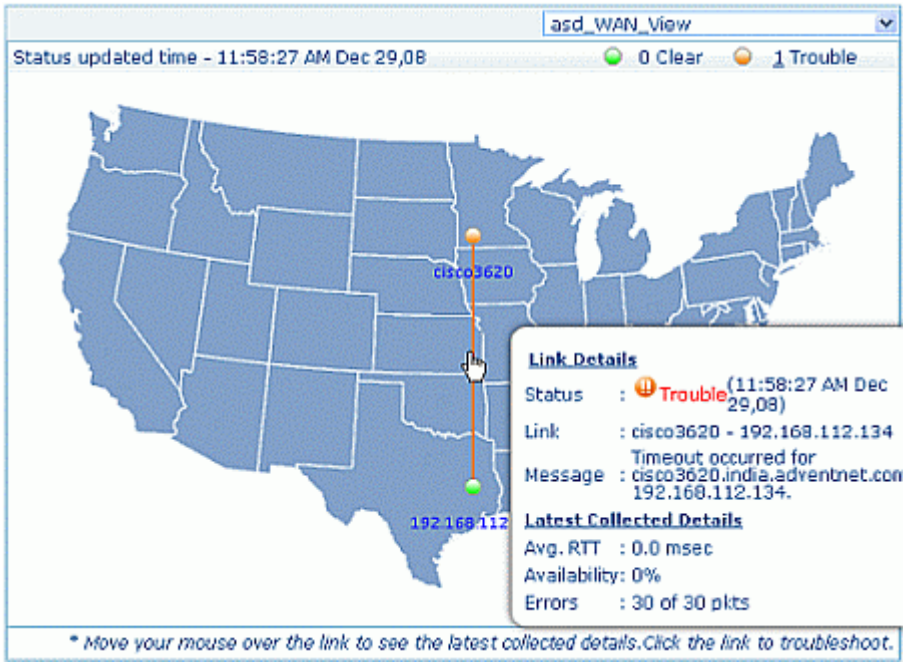
Defining Threshold for Round Trip Time

You can define a threshold template so that you are alerted with the WAN monitor violates a specified value. Here are the steps to define a threshold template:

1. Go to WAN Monitors > Settings page> Threshold Template.
2. Configure the upper and lower threshold limits for Round Trip time in msecs, the range being 0 to 60000 msecs. You can also choose various notification profiles configured in OpManager to alert you.

Business Views in WAN Monitor

In WAN Monitor, business views help you to know the status of the device and WAN link between devices at a glance. Whenever a new WAN monitor is created, a business view (image shown below) of it also gets created automatically with the default background and device icons. However, later you can modify the background and device icons if required.



In the business view, mouse-over the device icon or name/IP and WAN link to view its details. Clicking on the device icon will open the snapshot page of the device. Clicking on the WAN path opens the snapshot of the WAN path if it is in Clear state else opens the Hop graph in order to trace the fault to the exact hop.

Accessing WAN Monitor Business Views

1. Mouse-over **Maps** tab and select **WAN Monitors**.
2. Select the required business view from the drop down menu available on the top the business view displayed under the **Overview** tab.

Viewing WAN Monitor Alerts

Go to Maps-> WAN Monitor-> Alerts to view the alerts raised by WAN Monitor. All the alarms are listed with the Source name, Alarm Message, Status of the Device, Technician, Device category, date and time. Click the alarm message to view the alarm history.

Viewing WAN Monitor Reports

The WAN Monitor reports help you to view the reports on RTT threshold violation, RTT trend, Top N paths with Maximum RTT etc. to determine the health of the WAN links. To generate the WAN monitor reports, follow the steps given below:

1. Go to Reports-> WAN Monitor.
2. Click on the required report.

The generated report can be emailed or exported to a PDF version by click the respective icons on the report.

FAQs on WAN Monitor

1. Why there are no alerts from the device?

You might not have received alerts from the device if the trap host is not configured in the source Router. Make sure you configure the routers to send traps to OpManager. Telnet the router and type the following command:

snmp-server host <opmanager server IP> traps <host community string> rtr

For instance, if the OpManager host IP Address is 192.168.18.128, and the community string is private, the command would be:

snmp-server host 192.168.18.128 traps private rtr

2. Why should i give Snmp Write community to the router?

Both, the SNMP read and write community string needs to be set on the source router. The write community is used to configure the IPSLA agent on the device while the read community is used by OpManager to gather performance data from the router.

3. Why I am getting 'Source router SNMP write community may be wrong' error message?

OpManager uses SNMP to gather data from the Cisco IP SLA agent. This error is displayed when wrong SNMP read / write community string is configured for the Source router of the WAN Monitor in OpManager.

To configure the correct SNMP write community string in OpManager, go to the snapshot page of the source router and change the SNMP credentials by clicking on the '**Click here to change**' corresponding to the "**Passwords**" field. In the pop-up enter the appropriate credentials and submit it. After successfully submiting the correct SNMP credentials, try to add the WAN Monitor again for the Source device (Maps > WAN Monitor > Settings).

NCM Plug-in

About NCM Plug-in

The Network Configuration Management (NCM) plug-in a complete solution for easily Network Change and configuration Management. It offers multi-vendor network device configuration, continuous monitoring of configuration changes, notifications on respective changes, detailed operation audit and trails, easy and safe recovery to trusted configurations, automation of configuration tasks and insightful reporting.

The NCM plug-in manages network devices such as switches, routers, firewalls, wireless access points, integrated access devices etc., from multiple vendors. It imports the network devices from OpManager, builds up an inventory database and allows IT administrators to take control of configuring the devices from a central console. The added advantage with the NCM plug-in is that no need to again configure users and mail servers, the configuration that are made in OpManager itself is sufficient.

Installation Platfrom:

NCM plug-in supports only Windows installations as of now.

Database:

NCM plug-in uses the same MySQL bundled with OpManager.

Ports Used:

- Syslog: 519
- Web: 6060
- TFTP: 69
- SSHD: 22
- MySQL: 13306

Features:

- Multi-vendor configuration for switches, routers, firewalls and other devices
- Real-time configuration tracking and change notification
- Effective Change Management Policies
- Quick restoration to trusted configurations through a few simple steps

  Templates for commonly used configurations
  Automation of important device configuration tasks
  Encrypted storage of device configuration in database
  Contextual, side-by-side comparison of altered configuration
  Examining device configurations for compliance to a defined set of criteria/rules
  Comprehensive Audit Trails
  Detailed reports on inventory and configuration changes

Note:

Support for LDAP, RADIUS & Active Directory are disabled in this plug-in.

Installing NCM Plug-in

Download the NCM plug-in from OpManager website and follow the procedure given below to install:

1. Download OpManager's NCM plug-in file to OpManager server.
2. Shutdown OpManager Service.
3. Double click OpManager's NCM plug-in exe file. (You have to install NCM plug-in in OpManager server only)
4. Follow the on-screen instructions to complete the installation process.
5. Start the OpManager Service.

Note: You should have OpManager 8000 build or later.

Coniguring MySQL Server

NCM plug-in uses the same MySQL bundled with OpManager. However, if you are running any other MySQL (other than OpManager's) on the port 13306, NCM plug-in fails to connect to that MySQL and therefore the NCM server (DeviceExpert server) does not start up. If you wish to use the MySQL other than OpManager's running on the port 13306, follow the below procedures:

1. In <DeviceExpert_Home>/conf/Persistence/persistence-configurations.xml, change the value for the configuration parameter "StartDBServer" to 'false' as shown below: (default value 'true')
   <configuration name="StartDBServer"value="**false**"/>
2. Also in your MySQL, creat a database with the name "deviceexpert".
   Use the following command to create the database
   mysqladmin -u root -P 13306 create <databasename>
   (Here, 13306 denotes the MySQL port in DeviceExpert)

Importing Devices to DeviceExpert

Pre-requisite

The pre-requisite to import devices to DeviceExpert is that the devices must be discovered in OpManager.

Importing Devices to DeviceExpert

To import the devices to DeviceExpert follow the steps given below:

1. From OpManager, click on the Network Configuration Management link available in the header. Or From DeviceExpert, click Inventory tab. The inventory page opens
2. Click on Import tab and select Import devices, if the device is SNMP enabled or click on Import SNMP devices.

Use the **Import SNMP Device** option to import the devices that are SNMP enabled (except Desktops) as DeviceExpert itself takes care of everything right from configuring the Device category to identifying the serial and model numbers. Whereas, you can use **Import Device** option to import the Desktops that are SNMP enabled and other devices that are not SNMP enabled. In this case you need to manually enter the serial and model numbers.

Import Device:

1. Select the Host Name/IP Address, Vendor and Device Template Name of the device that is to be imported.
2. Specify its Serial and Model numbers.
3. Click Add.

Import SNMP Device:

1. Select the devices that are to be imported from the left column and move to the right column.
2. Click Import.

The devices are imported into DeviceExpert.

Providing Credentials for Devices

Contents

Overview

Once you add the device to the DeviceExpert inventory, you need to provide device credentials to establish communication between the device and DeviceExpert. Details such as the mode (protocol) through which communication is to be established, port details, login name, password etc. are to be provided.

Guidelines on choosing credentials for a Single Device

To establish credentials for a single device,

1. Go to "Inventory" and select the device for which communication has to be established
2. click 'Credentials' menu on the top bar

In the Credentials UI, provide the following details:

Choosing the Protocol

Based on the type of device, you can select any of the following combinations of protocols to establish communication between DeviceExpert and the device:

1. **TELNET-TFTP** (Establishing communication with the device via Telnet and transferring the configuration via TFTP)
2. **TELNET** (Establishing communication with the device via TELNET and executing show commands on the device to get configuration details)
3. **SSH-TFTP** (Establishing communication with the device via SSH and transferring the configuration via TFTP)
4. **SSH-SCP** (Establishing communication with the device via SSH and transferring the configuration via SCP)
5. **SSH** (Establishing communication with the device via SSH and executing show commands on the device to get configuration details)
6. **SNMP-TFTP** (Establishing communication with the device via SNMP and transferring the configuration via TFTP)

Based on the protocol choice, you need to provide other credentials.

For TELNET-TFTP, TELNET, SSH-TFTP, SSH-SCP & SSH

User Credential Profile

If you have downloaded DeviceExpert and carrying out the settings for the first time, you may skip this 'User Credential Profile' step.
DeviceExpert offers the flexibility of creating common credentials and sharing the common credentials among multiple devices. The Common Credentials are known as profiles. For more details click here.

Credentials for TELNET-TFTP, TELNET, SSH-TFTP, SSH-SCP & SSH

The following screenshots depict how to enter the credentials for the devices. For ease of understanding, the screenshots illustrate how the credentials are entered while accessing the device via a telnet console and explain how the same values are entered in the DeviceExpert GUI.

Credentials have been split into two divisions:|

Primary Credentials - deal with parameters that are necessary to establish communication with the device. Details such as Login Name, Password, Prompt, Enable UserName, Enable Password and Enable Prompt are classified as basic details.

Additional Credentials - certain parameters usually take standard values. All such parameters have been classified under 'Additional Credentials'. Port, login prompt, enable userprompt, password prompt, enable password prompt values are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details. Providing **TFTP Server Public IP / SCP Server Public IP** if the device is behind NAT/firewall has also been classified under Additional Credentials.

Important Note: Refer to the explanatory screenshots below before proceeding with entering the credentials.

Primary Credentials

S.No	Credential	Description
1	Login Name	While establishing connection with a device, if the device asks for a Login Name, set a value for this parameter. This parameter is Optional.
2	Password	To set the Password for accessing the device.
3	Prompt	The prompt that appears after successful login.
4	Enable UserName	When entering into privileged mode, some devices require UserName to be entered. Provide the username if prompted; otherwise leave this field empty.
5	Enable Password	This is for entering into privileged mode to perform configuration operations like backup/upload. This parameter is mandatory.
6	Enable Prompt	This is the prompt that will appear after going into enable mode.

Additional Credentials

Click the link "Additional Credentials" to view/enter values for these parameters. Except TFTP/SCP Server Public IP, all other parameters are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details.

S.No	Credential	Description
1	TFTP / SCP Server Public IP	When the device is present outside the private network (i.e. when the private IP of DeviceExpert is not reachable for the device) this parameter can be used to provide the public IP of the DeviceExpert server (NAT'ed IP of DeviceExpert). This IP will be used in Configuration backup via TFTP / SCP.
2	Telnet/SSH Port	Port number of Telnet/SSH - 23 (for Telnet) and 22 (for SSH) by default.
3	Login Prompt	The text/symbol that appears on the console to get the typed login name is referred as login prompt. For example, Login**:**
4	Password Prompt	The text displayed on the console when asking for password. For example, Password**:**
5	Enable User Prompt	The text displayed on the console when asking for Enable UserName. For example, UserName**:**
6	Enable Password Prompt	The text displayed on the console when asking for password. For example, Password**:**

After providing the credentials, if you want to take a backup of the device immediately after updating the credentials, select the 'backup' checkbox
Click 'Save & Test' if you want to test the validity of the credentials; otherwise, click "Update" to apply the values
The chosen credentials would be applied to the Device

Once you complete this step - that is, providing credentials, you will find the credentials icon beside the device name in the inventory.

For SNMP-TFTP

User Credential Profile

If you have downloaded DeviceExpert and carrying out the settings for the first time, you may skip this 'User Credential Profile' step.

DeviceExpert offers the flexibility of creating common credentials and sharing the common credentials among multiple devices. The Common Credentials are known as profiles. For more details click here.

Primary Credentials for SNMP-TFTP

S.No	Credential	Description
1	SNMP Port	Port number of SNMP - 161 by default.
2	Read Community	An SNMP community is a group of managed devices and network management systems within the same administrative domain. Each SNMP request packet includes a community name. When a request packet is received, the remote access server looks for the name in its community table: If the name is not found, the request is denied and an error is returned. If the name is found, the associated access level is checked and the request is accepted if the access level is high enough for the request. The SNMP Read Community string is like a user id or password that allows Read-only access to the device.
3	Write Community	The SNMP Write Community string is like a user id or password that allows Read and Write access to the devices.

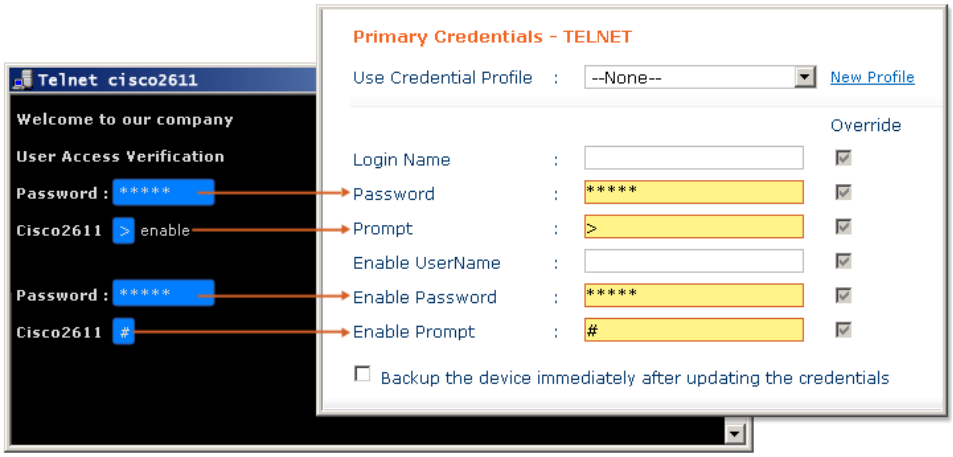
Additional Credentials

Click the link "Additional Credentials" to view/enter values for these parameters. Except TFTP/ SCP Server Public IP, all other parameters are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details.

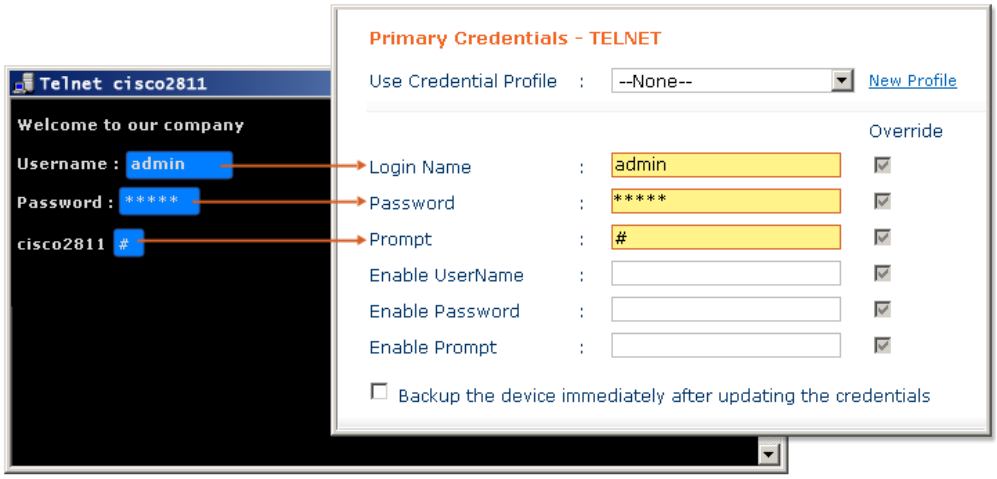
S.No	Credential	Description
1	TFTP / SCP Server Public IP	When the device is present outside the LAN (i.e. when the private IP of DeviceExpert is not reachable for the device) this parameter can be used to provide the public IP of the DeviceExpert server (NAT'ed IP of DeviceExpert). This IP will be used in Configuration backup via TFTP.

Explanatory Screenshots

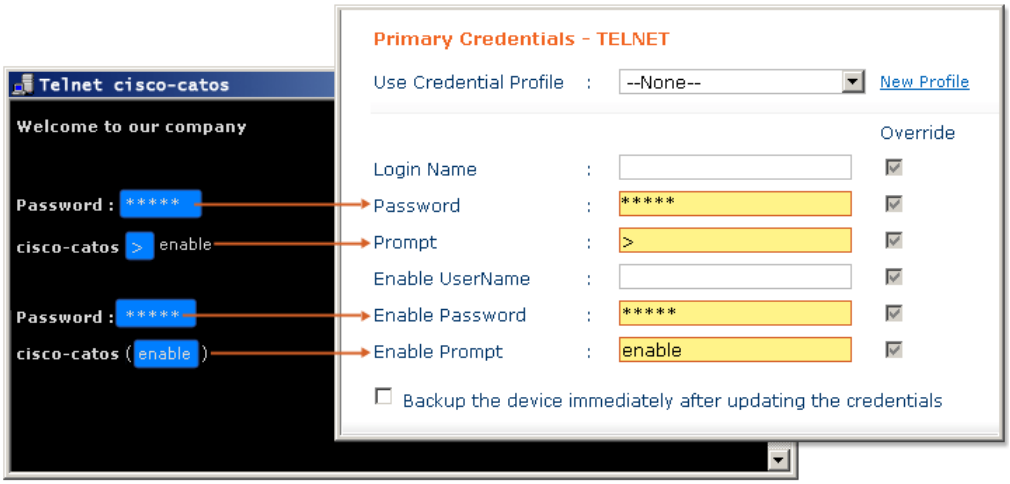
Example 1: Cisco IOS Device - Password and Enable Password configured.



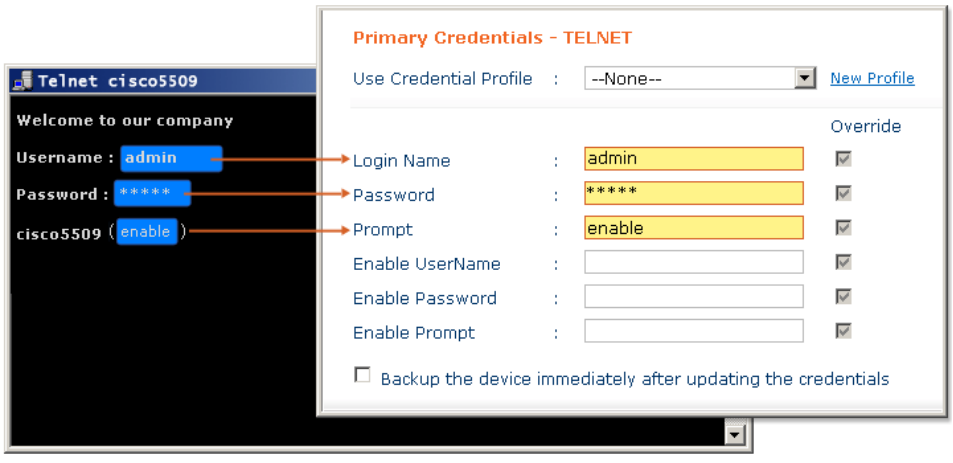
Example 2: Cisco IOS Device â€“ Directly going to Enable Mode



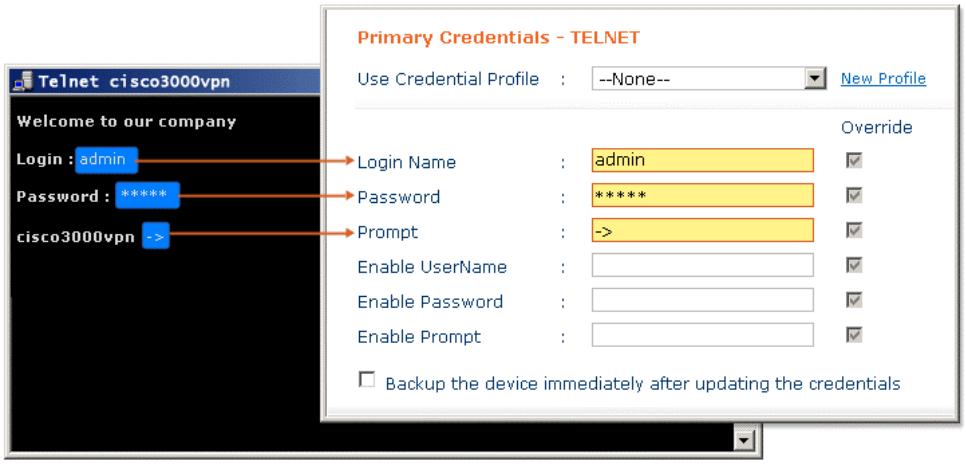
Example 3: Cisco CatOS Device - Password and Enable Password configured.



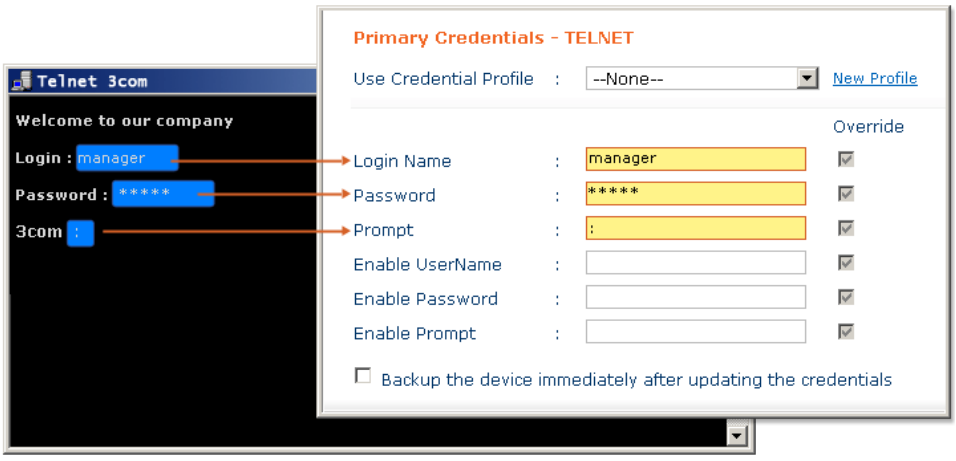
Example 4: Cisco CatOS Device â€“ Directly going to Enable Mode



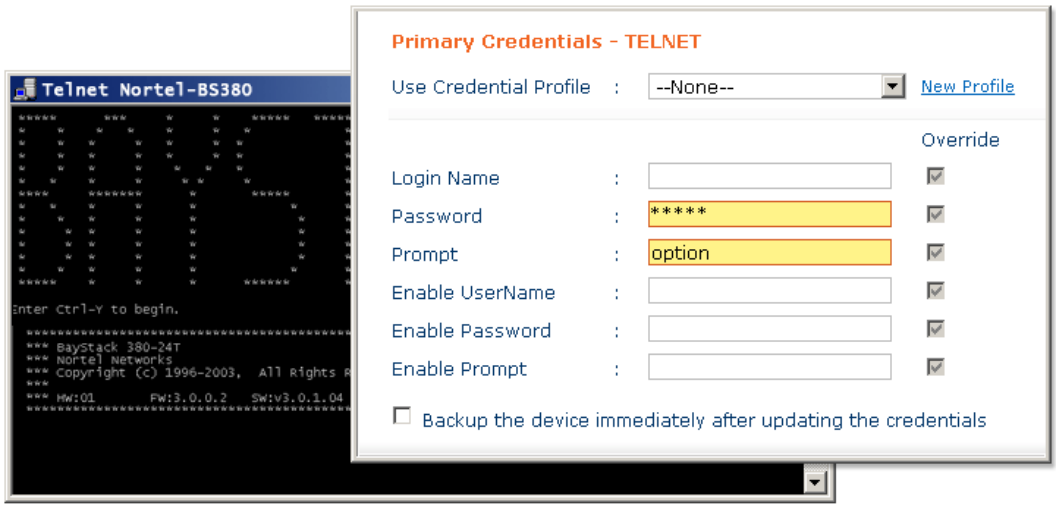
Example 5: Cisco VPN Concentrator



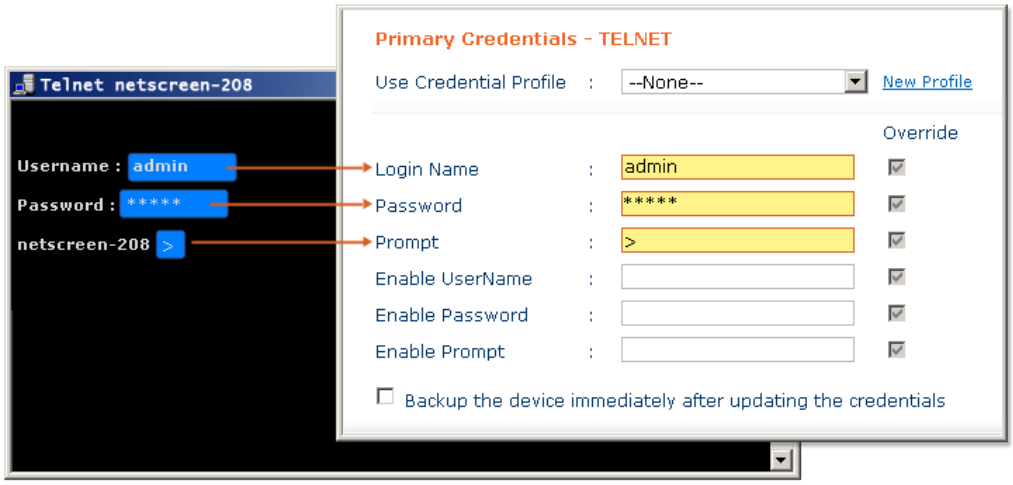
Example 6: 3Com Router



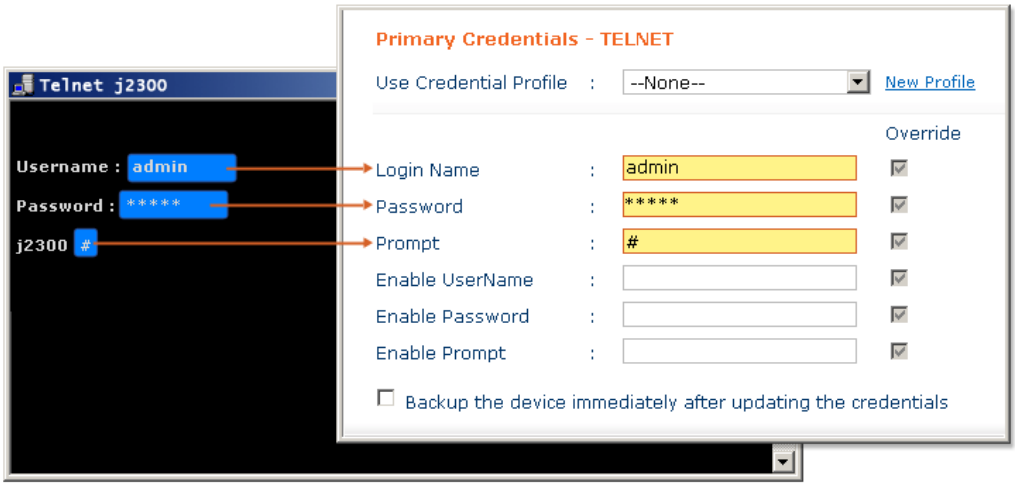
Example 7: Nortel BayStack



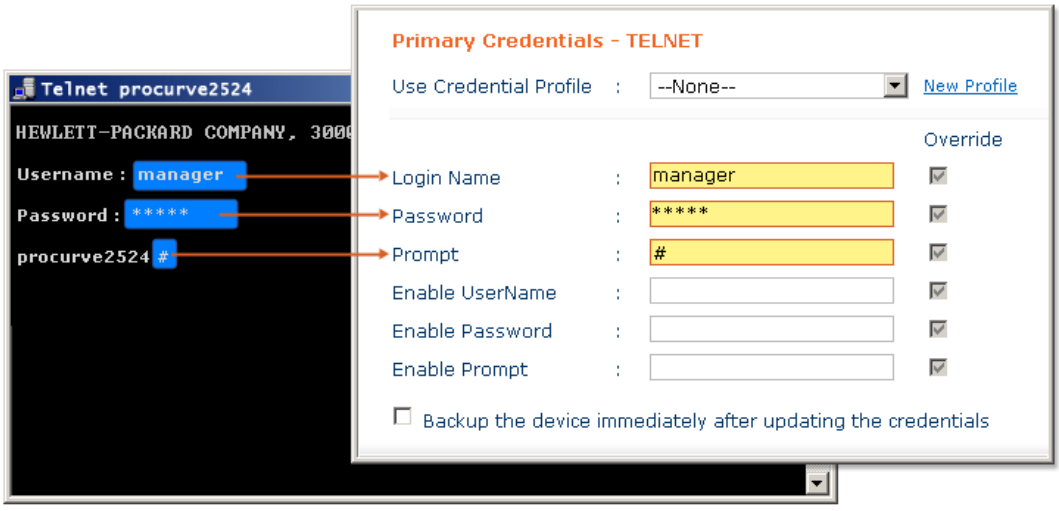
Example 8: NetScreen Firewall



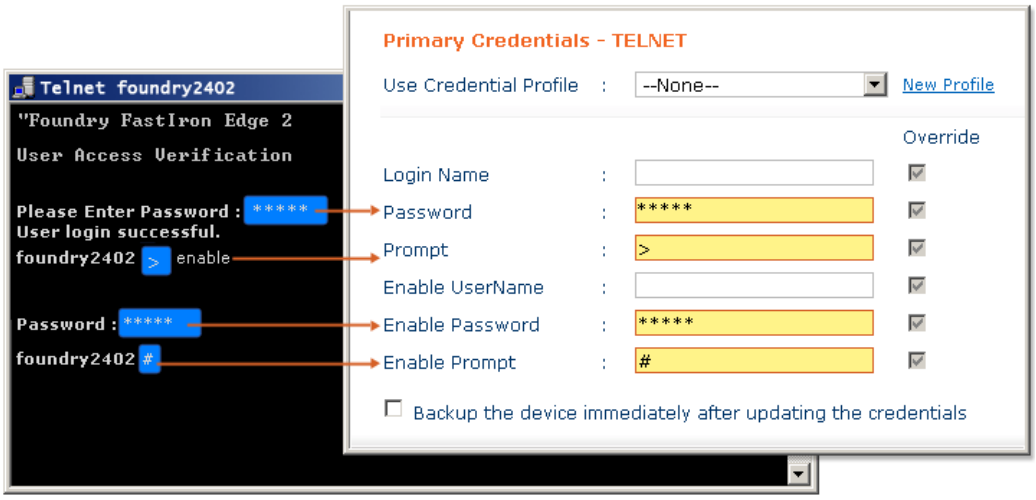
Example 9: Juniper Router



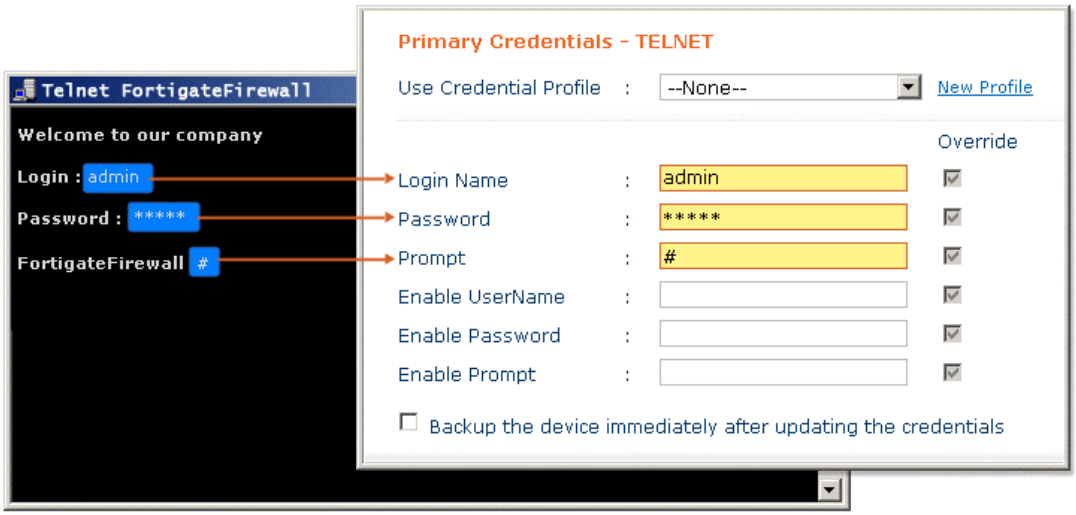
Example 10: HP Procurve Switch



Example 11: Foudry Switch



Example 12: Fortinet Fotigate Firewall

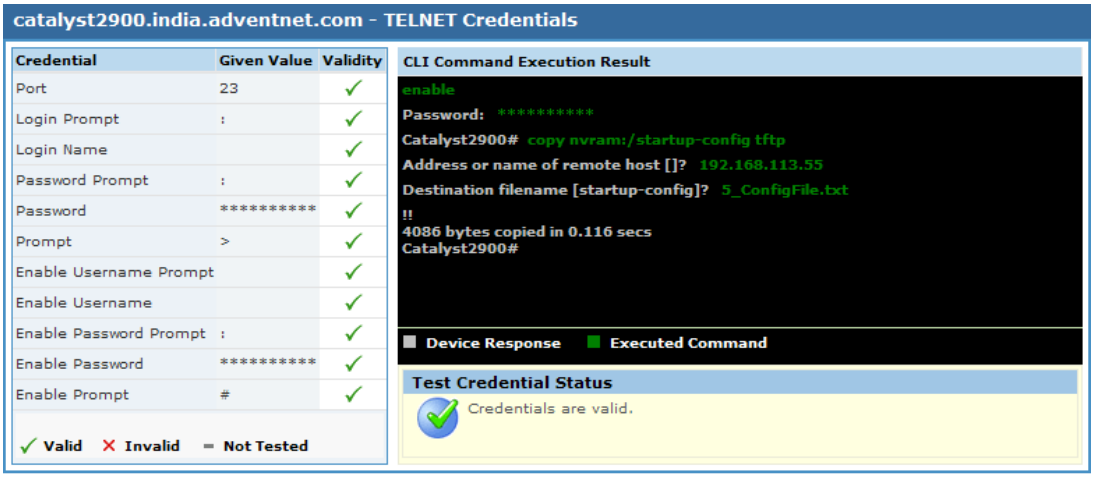


Testing the Validity of Credentials

Credential values entered through the Credentials GUI should be accurate. Otherwise, DeviceExpert will not be able to establish connection with the device. To ensure the correctness of credential values, DeviceExpert provides the testing option. After entering the credentials, you can test the values during which DeviceExpert will indicate if the values entered are valid. It will pinpoint the invalid values and you can carryout corrections accordingly.

To test the validity of credentials,

After providing the credentials, click 'Update & Test'
This updates the credential values in the DB and then carries out the testing. The result of the testing will be shown in a separate window as below:



The testing result indicates valid credential values with a green 'tick' mark. The invalid values are marked as red cross marks. You need to change the invalid values. Alongside, the CLI command execution result (through which DeviceExpert ascertains the validity of credential values) is also displayed
If you want to test the validity of credentials of a device which has already been given credentials, select the particular device in the inventory, click 'Credentials'. In the Device Credentials page that opens up, click "Test Credentials". Rest is same as above.

Note: The credential testing option is provided only for TELNET-TFTP, TELNET, SSH and SSH-TFTP protocols.

Sharing Common Credentials Across Devices

In practical applications, you may find that the same set of credentials could well be applied 'as they are' to many devices. In such cases, to avoid the cumbersome task of entering the credentials for each device separately, DeviceExpert offers the flexibility of creating common credentials and sharing the common credentials among multiple devices. This is called as 'Credential Profile'.

Credential Profile can be created as a ready-to-use format called simply as 'Profiles'. You can create a profile with a specific name. Once you create a credential profile, its name will automatically be listed in the drop-down menu in the "Credentials" UI for the field "Use Profile". When you wish to use the profile, if you just choose the corresponding profile in the drop-down menu, all the credential information will be automatically filled-up.

Creating Credential Profiles

To create Credential Profiles,

Go to **"Admin" >> "Device Management" >> "Credential Profile" >> "New Profile"** (Alternatively, you can click the "Add New" action item present beside the 'Use profile" drop-down in the **Inventory ---> Credentials** GUI).
In the 'Add Credential Profile' GUI that opens,

Provide a Name for the new credential profile that has to be created. This is the name that will appear in the "Use Profile" drop-down
Provide a description for the profile. Though this is for reference purpose, filling up this field is mandatory to avoid confusion at any future point of time
Fill-up credential values for the desired protocol. [Refer to the description provided above for information about the parameters and guidelines on choosing the values] and click the "Add". The New Credential Profile is created

Managing Credential Profiles

Go to **"Admin" >> "Device Management" >> "Credential Profile"** to edit/remove a profile or to view the devices referred by a profile.

Device Groups

Contents

Overview

Sometimes, you might need to group devices based on some logical criteria. For example, you may wish to create groups such as a group containing all cisco routers, or a group containing all cisco switches etc., This would help in carrying out certain common operations with ease. A group can be based on some criteria or could be just a random collection of devices. This section explains how to group devices and perform various operations in bulk for the group as a whole.

Creating Device Groups

1. Go to **"Inventory" >> "Device Group"** and click "**New Group**"
2. In the UI that comes, provide a name and description for the new group
3. The group should be assigned with devices. To associate devices with the group, select "**By Specific Device**" to simply select the needed devices from the list and form a group;
4. Choose "**By criteria**" if you want to group the devices based on criteria such as IP, Manufacturer, Model, Device Type and OS Type. Whenever a new device matching the criteria specified is added to the DeviceExpert inventory, it automatically becomes part of the group
5. Device Groups can be created as '**Public**' or '**Private**'.

   By default, the groups are created as private groups - that means, only authorized users will be able to view the group.
   On the other hand, if you have a requirement to make certain groups visible to all, you can create the group as a 'Public Group'.
   If you select the checkbox "**Make it as Public Group**", the group will be created as a public group.
   All users, irrespective of their roles, would be able to view the group.
   However, the device access restrictions for and 'Operators' will not be affected - that means, though they can view the public group, they will be able to access only those devices that have already been assigned to them within the public group.
   Public groups, once created, cannot be reverted to private.

6. Click "**Save**"

Once you create a group, the name of the group will be listed under "Device Group" in the left pane.

What are the operations one can perform on Device Groups?

DeviceExpert supports the following operations to be performed for Device Groups:

1. Setting Credentials for all the devices of the group
2. Configuration Backup for all devices of the group at one go
3. Configuration Upload for all devices of the group in bulk
4. Configuration change management for all devices of the group
5. Defining compliance rules/policies for all devices of the group

Performing operations on a group

1. Go to **"Inventory" >> "Device Group"** and click the name of the group. Upon clicking this, the Associated Devices would be listed
2. Perform any operation as desired by choosing the relevant menu item

Managing Device Groups

Editing a Group

You can change any information pertaining to a particular group. For instance, you can change the group name, edit the description or modify the criteria. To do any or all of these tasks,

1. Go to **"Inventory" >> "Device Group"** and click the "Edit" link present against the group to be edited
2. Change the desired field and click "Save"

Removing a Device Group

1. Go to **"Inventory" >> "Device Group"** and click
2. click the "trash bin icon" before the name of the group to be deleted. The group will be deleted once and for all.

Note: If the device group you are trying to delete is referred by some other operation such as a Schedule, you will not be able to delete the group until all the references are removed.

Managing Configurations

Backing up Device Configuration

Contents

Overview

After setting up the devices, the first operation that would be performed is backing up the device configuration. Backup could be done anytime on demand for a single device or a group of devices in bulk. It can also be automated by creating scheduled tasks.

Important Terms

Backup Operation denotes retrieval of current configuration from device and transfer of the same to DeviceExpert
Upload Operation denotes the transfer of the selected configuration from DeviceExpert to the device

Where do you store the backedup configuration files?

The backedup configuration files are stored in the DeviceExpert database in encrypted form. The configuration can be viewed from the "Device Details" page in the GUI.

Taking Backup of Device Configuration

Prerequisite

Before proceeding to backup device configuration, you should have provided credentials for the device. The credentials should be valid so that the DeviceExpert is able to communicate with the device.

To take immediate Backup,

1. Go to "**Inventory" >> "All Devices" >> Select the device or devices** whose configuration has to be backedup
2. Click the button "**Backup Config**"
3. Once backup is over, the status will be marked as "Backedup" with a green tick mark. If the operation fails, a red cross mark is displayed.

Note:
(1) Backedup version will be stored in DeviceExpert only if there is a difference between currently available configuration in the device and the previously backedup version. Otherwise, it is not stored
(2) When the Backup operation fails, you can find the reason why it failed, by clicking the status of the operation in the inventory page - that is, by clicking the link "Backup Failed' present under the column 'Operation' in the inventory. Alternatively, you can click the same link in the under the column 'Error Info' in 'Operation Audit' page

Automating backup through schedules

You can automate device configuration backup by creating schedules. The backup can be generated at periodic intervals. Refer to scheduled tasks section for more details.

Viewing Device Configuration Details

Contents

Overview

After adding the device and providing the credentials, the details about the device can be obtained from the inventory tab in the GUI. This section explains how to view various details about the device and viewing the device configuration.

Viewing Devices

The devices added to DeviceExpert can be viewed from the "**Inventory >> All Devices**"

Viewing Device Details

Pre-requisite

To view device details/configuration, you should have supplied device credentials properly

Device Details

The Device Details are presented in three sections:

1. **Basic device properties** (hostname, IP, device status, operation status etc.,)
2. **Hardware properties** (device type, make, model, chassis details etc.,)
3. **Configuration Details** (current configuration, history of changes in configuration etc.,)

Viewing Basic Device Properties

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose properties are to be viewed
2. In the GUI that opens up, the device properties are displayed on the LHS

Hardware Properties

Upon giving credentials and taking backup of device configuration, hardware properties of the device such as chassis details, model number could be fetched and displayed on the device details page.

To view the hardware properties,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose hardware properties are to be viewed
2. In the GUI that opens up, click the tab "**Hardware Properties**" the device properties are displayed on the LHS

Note: Every time device configuration backup is done, the hardware properties are also fetched and updated. At any point of time, you wish to fetch harware properties, simply execute device backup.

Viewing Device Configuration

One of the important functions of DeviceExpert is retrieving the configurations from devices and storing them with proper versions in the database. At any point of time, you can view the current version or any of the previous versions of the configurations. This can be done from the 'Device Details' page.

Before proceeding further, it is pertinent to look at the definitions of the following terms:

Current Configuration: this reflects the currently available configuration in the device
- **Current Startup Configuration:** this reflects the currently available startup configuration in the device - this is, the configuration that will be loaded when the device starts up
- **Current Running Configuration:** this reflects the currently available running configuration in the device

Startup History: History of changes that were done over the Startup Configuration. This is presented in terms of change versions in hierarchical order

Running History: History of changes that were done over the Running Configuration. This is presented in terms of change versions in hierarchical order

Baseline Configuration: The Baseline configuration refers to a trusted working configuration. You can keep any version of device configuration as the Baseline Configuration. When you want to revert to a safe configuration version or while doing disaster recovery, Baseline configuration would come in handy

Labelled Configuration: For any version of configuration, you can associate a label - that is, a unique tag. As configuration versions keep on changing, you will have difficulty in remembering the version number of a particular good configuration. To avoid that, you can associate the version with a label for easy identification

Draft Configuration: As the name indicates, this is a new configuration created by you. For creating a draft configuration, you can take up any version of device configuration - startup or running - and save it as a draft as it is or after carrying out some changes. You can also create a new draft altogether

Viewing Current Version (Running & Startup)

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be viewed
2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**Current Version**" against "**Running Configuration**" / "**Startup Configuration**" whichever is required

Viewing Baseline Version (Running & Startup)

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be viewed
2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**Baseline Version**" against "**Running Configuration**" / "**Startup Configuration**" whichever is required

Viewing History of Running/Startup Configuration

The history of changes that were done over the Running/Startup Configuration are listed with version numbers representing the change. In addition, other details such as who effected the changes at what time and also the reason for the change are also listed.

To view the running configuration history,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be viewed

2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**Current Version**" against "**Running Configuration**" / "**Startup Configuration**" whichever is required
4. In the GUI that opens up, the current configuration is shown. The drop-down against the field "**Configuration Version**" provides the list of all configuration versions. Select the required version. It will be shown in the GUI.

Managing Configurations

Editing Configuration Files

You can choose any version in the startup/running history and edit them as draft.
To edit configuration files,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be edited
2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**Current Version**" against "**Running Configuration**" / "**Startup Configuration**" whichever is required to edited
4. In the GUI that opens up, the current configuration is shown. The drop-down against the field "**Configuration Version**" provides the list of all configuration versions. Select the required version. It will be shown in the GUI.
5. Click "**Edit as Draft**" available in the drop-down under "**Actions**". You may now edit the content. Click "**Save**". You may upload it to the device immediately (as startup/running configuration) by clicking the link "**Upload**" in "**Actions**"

Creating New Drafts

Instead of editing the startup/running configuration, you can create fresh draft configuration to pload only a few commands - say for updating SNMP community.

To create a draft,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be edited
2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**New Draft**" against the field "Drafts for this device"
4. In the text editor that opens up, you can create the draft with the required commands and "**Save**". You may upload it to the device immediately by clicking the link "**Upload**" in "**Actions**". You may upload it to the device immediately (as startup/running configuration) by clicking the link "**Upload**" in "**Actions**"

Important Note: When you upload a new draft to the running configuration of a device, the difference is merged with the previous version. On the other hand, when it is done on the startup configuration, only the draft contents are uploaded - that means, the previous version will be replaced by the draft contents. So, exercise care while uploading draft to the startup configuration.

Comparing Configuration Versions

One of the powerful features of DeviceExpert is its capability to provide side-by-side difference between any two configuration versions. You can compare two configuration versions of the same device or of different devices.

To compare configurations,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device whose configuration is to be compared

2. In the GUI that opens up, the configuration details are displayed on the RHS
3. Click the link "**Current Version**" against "**Running Configuration**" / "**Startup Configuration**" whichever is required
4. In the GUI that opens up, the current configuration is shown. The drop-down against the field "**Configuration Version**" provides the list of all configuration versions. Select the required version, which is to be compared with another version.
5. Go to "Show Difference" button and select an option from the drop-down (Diff with Previous, Diff with Baseline, Diff with Startup/Running, Diff with Any)

Performing Various Actions on Devices/Configurations

From the **"Inventory" >> "Device Details"** page, you can perform various actions on the device such as enabling real-time configuration change detection, executing various 'show' commands on the device, edit device properties, edit credentials and launching telnet connection with the device.

Executing 'show' commands

You can execute 'show' commands such as '**Show Version**', '**Show Interfaces**', "**Show Tech Support**", "**Show Access Lists**", "**Show Logging**", "**Show IP Traffic**" and "**Show Buffers**" on specific devices from the inventory tab. DeviceExpert executes the command and displays the result.

To execute 'show' commands,

1. Go to "**Inventory >> All Devices**" and click the hostname of the particular device on which the show command is to be executed
2. Go to "**Actions**" and click the link "**Show Commands**" in the drop-down. The various commands that are applicable for the selected device, are displayed. Click the desired command. The result of the command is displayed in a new window

Note: If you want to execute show commands on multiple devices at one go, make use of the script execution in configuration templates.

Enabling Real-time Change Detection

Refer to the section Real-time change detection

Establishing Telnet Connection

You can launch telnet connection with the device from the Device Details page. Once you provide the credentials needed, you would be able to have a telnet console and work with it.

To launch telnet connection,

Go to "**Inventory >> All Devices**" and click the hostname of the particular device for which you wish to open a telnet session

- Go to "**Actions**" and click the link "Telnet"
- In the UI that opens up, provide the following credentials:

Remote Host: The host to which the session is to be established
Remote Port: The default is set for telnet(23)
Login Name: One of the user name/login name present in the remote host
Password: Password for the user
Login Prompt: This is the prompt that the device issues for getting the user name
Password Prompt: This is the prompt that is issued by the device for getting

the password **Command Prompt:** This is the prompt displayed by the device for each command

- Click "**Connect**"
- Telnet console would be launched

Switch Port Mapper

DeviceExpert provides the 'Switch Port Mapper' tool that helps network administrators identify the list of devices connected to each port of the managed switch. This eliminates the need for manually tracing the network cables.

The tool discovers the devices plugged into each port of a specified switch. It helps in gaining visibility into the IP, MAC, VLAN, status and availability of ports. Total number of ports, total number of available ports, total number of transient ports are all provided. Since this is a real-time discovery, the administrators can also view the operational status and speed of each port. At any point of time, you can execute the tool to view the mapping.

Prerequisite:

To execute switch port mapper, you should have entered SNMP credentials through SNMP profiles. If you have not created any SNMP profile, create one before proceeding further.

To execute 'Switch Port Mapper',

1. Go to "**Inventory" and** click **"Actions"** button present at the RHS of the table against the hostname of the particular device for which you wish to find 'switch port' mapping
2. Click the link "**Switch Port Mapper**" in the drop-down
3. In the UI that opens up, the mapping details are displayed. If you want to run it afresh, click "**Scan Switch Port**" again

Note: Switch port mapping is applicable only for the SNMP-enabled devices. If you want to change the SNMP community, you can do that from the above UI that displays the mapping.

Uploading Device Configuration

Contents

Overview

While backup deals with taking a copy of the device configuration and retaining it in the DeviceExpert, Upload refers to the opposite. "Upload" transfers the configuration from DeviceExpert to device. Entire configuration file or even select lines/snippet within a file can be uploaded using DeviceExpert.

Uploading Full Device Configuration

1. Go to "**Inventory**" >> Click the device whose configuration has to uploaded
2. In the Device Details UI that opens up, go to the "**Device Configuration**" section and click "**Baseline Version**" of Running/Startup configuration as per your requirement
3. In the GUI that opens up, from the "Configuration Version" drop-down, you can select and view any configuration version.
4. Select the version to be uploaded, check the configuration and click "Upload" available in the drop-down "Actions"
5. The selected version of the configuration will be uploaded to the device

To Upload Select Lines of Configuration to a Single Device

1. Go to "**Inventory**" >> Click the device whose configuration has to uploaded
2. In the Device Details UI that opens up, go to the "**Drafts for this device**" section and click "**New Draft**"
3. In the GUI that opens up, if required, you can refer to the startup/running configuration of the device
4. Enter the command sets/lines that are to be uploaded to the device configuration
5. Click "Save" and then go to "**Actions >> Upload**". In the UI that pops-up, select the configuration type to which you wish to upload the draft - 'Startup' or 'Running'

To Upload Configuration Snippets

Refer to the section 'Automation using templates & scripts'

Uploading Configuration to Multiple Devices

DeviceExpert provides the option to upload labelled configuration to multiple devices/device groups at one go. The devices or device groups should have a common label. For example, all devices will have the 'BASELINE' label. You can upload the contents of the 'BASELINE' label to all the devices at one go. Entire content in the respective 'BASELINE' version would be uploaded to the respective device.

Selecting Multiple Devices

1. Go to "**Inventory**" and select the devices whose configuration has to uploaded
2. Click the button "**Upload Config**"
3. In the GUI that opens up, the common labels shared by the devices are displayed. Select the required label and click "**Upload**"

Real-time Configuration Change Detection

Contents

Overview

Unauthorized configuration changes often wreak havoc to the business continuity and hence detecting changes is a crucial task. Detection should be real-time to set things right. DeviceExpert provides real-time configuration change detection and this section explains the steps to be done for enabling change detection.

How does real-time change detection work?

Many devices generate syslog messages whenever their configuration undergoes a change. By listening to these messages, it is possible to detect any configuration change in the device. DeviceExpert leverages this change notification feature of devices to provide real-time change detection and tracking.

How does real-time detection benefit me?

This comes in handy for administrators to keep track of the changes being made and to detect any unauthorized changes. By enabling this, you can

1. Capture configuration as and when changes happen
2. Get real-time notifications on change detection
3. Find information on who carried out the change and from where (the IP address)
4. Detect unauthorized changes on real-time

How do I enable real-time change detection?

You can enable change detection for a single device or for many devices at one go. Change detection can be enabled only for those devices for which you have provided the device credentials.

To detect configuration changes through syslog,

1. Go to the "**Inventory**" tab. Select the device or devices for which you wish to enable change detection
2. Click the link "**Enable Change Detection**" available in the drop-down under "**More Actions**" and fill-in the details

To disable configuration change detection,

In case, you wish to disable the already enabled configuration tracking, you can do so as follows:

1. Select the device or devices for which you wish to disable change detection
2. Click "**Enable Change Detection**" available in the drop-down under "**More Actions**".

3. In the UI that opens, click the option "**Disable**" for the parameter '**Detecting Config Changes through Syslog**'

How do I capture information on 'who changed' the configuration?

DeviceExpert captures username and IP address when someone opens a telnet console and directly carries out a configuration change to ***Cisco devices*.**

To capture this information, the following conditions are to be satisfied:

Login name should be enabled for cisco switches and routers and
syslog-based change detection has to be enabled (or) information on who changed the configuration should be present in the configuration header

When a user accesses the device via a telnet console and carries out any changes, the username will be captured under the "Changed By" column of the backedup configuration information. The IP address of the user will be printed in the annotation column.

Automated Change Detection through Schedules

Configuration change tracking can be scheduled through periodic configuration backup tasks. Configuration can be automatically backedup by adding a schedule and configuration versions can be tracked. For more details, refer to the 'Scheduled Tasks' section.

Troubleshooting Tips

Important Note

You may sometimes notice the following message in Syslog Configuration for Change Detection:
Device(s) not supporting Configuration Detection through Syslog
<device1>, <device2>, <device 3>
This message is displayed in any of the following scenarios:

- Device does not generate syslog messages; so syslog-based change detection is not possible
- Device generates syslog messages for configuration change events but DeviceExpert has not yet added change detection support for this device. If this is the case, contact support@opmanager.com
- In the case of Cisco IOS routers and switches, if SNMP protocol is used for communicating with the device, auto configuration for "syslog based change detection" is not supported. In such a case, you need to manually configure the router/switch to forward syslog messages to the DeviceExpert syslog server. Change Detection will then be enabled. Alternatively, you can choose Telnet as the protocol for communication

Configuration Change Management

Contents

Overview

Monitoring the changes done to the configuration is a crucial function in Configuration Management. DeviceExpert provides convenient change management options. Once the configuration change in a device is detected, it is important that notifications are sent to those responsible for change management. It also provides option to roll-back the changes.

DeviceExpert helps in sending notifications in four ways:

1. Sending Email
2. Sending SNMP Traps
3. Generating trouble Tickets
4. Rolling back to the previous version or the baseline version

And these notifications can be sent whenever there happens a change in

1. Startup or Running Configuration
2. Startup Configuration alone
3. Running Configuration alone

How to set up Change Management?

Setting up Change Management is a simple, three-step process:

1. Provide a name for the Change Management Rule
2. Choose Change Management condition
3. Specify the action

Providing a name for the Change Management Rule

This step deals with just providing a name and description for the intended change management rule. 'Change Management Rule' here refers to the condition based on which you would like to get the notification. As stated above, notification could be triggered when startup and/or running configuration of a device undergoes a change. You may provide names such as "Startup Config Changed', "Running Config Changed". This would be of help in identifying the rule and for reusing it for other devices later.

To provide a name,

1. Go to **"Inventory" >> "All Devices"** and click the name of the device for which change management has to be enabled
2. Click the tab "**Change Management**"
3. In the "**Change Management**" GUI that opens up, click the button "**New Rule**"
4. Enter '**Rule Name**' and '**Description**' in the respective text fields

Choosing Change Management Condition

Click any one of the radio buttons -

- Startup or Running Configuration is changed - to send notification when either Startup or Running configuration of a device is changed
- Running Configuration is changed - to send notification when the Running configuration of a device is changed
- Startup Configuration is changed - to send notification when the Startup configuration of a device is changed

Specifying the action

After defining the condition in the previous step, you can specify any of the following three actions:

1. **Sending Email** - sending Email notifications to the desired recipients
2. **Sending SNMP Traps** - sending an SNMP v2 trap to specific host
3. **Generating Trouble Tickets** - generate a trouble ticket to help desk
4. **Rollback Configuration** - to revert to the previous configuration version or to the baseline version

Sending Email Notifications

To send email notifications to the desired recipients (based on the change management condition specified earlier),

1. Click the checkbox "**Send Email Notification**"
2. Enter the Email ids of the intended recipients. If you want to send the notification to multiple recipients, enter the ids separated by a comma. By default, the Email ids configured through Admin >> Mail Settings page are displayed here. You may add new Email ids if required
3. Provide a subject for the notification and the actual message in the respective fields. Here, in the subject and message fields, you have the option to provide details such as Device Name, IP, type of configuration that underwent change (startup/running), and who changed the configuration
4. For this purpose, DeviceExpert provides replaceable tags - **$DEVICENAME, $DEVICEIP, $CONFIGTYPE and $CHANGEDBY**. You may use these tags to provide exact details in the subject and message fields of the notification.
   Example: $CONFIGTYPE of $DEVICENAME changed

   Explanation: If the $CONFIGTYPE is "Running Configuration" and $DEVICENAME is "Primary Router", the actual message in the notification would be "Running Configuration of Primary Router changed". These tags get replaced with the actual values at runtime.
5. You have the option to append the configuration diff in the message. The difference with the previous version would be pasted in the message field. To enable this option, click "**Append Configuration Difference in Message**". Click "**Save**".

Sending SNMP Trap

SNMP v2 traps could be sent to specific host upon detecting a configuration change. To send SNMP trap to the desired host (based on the change management condition specified earlier),

1. Click the checkbox "**Send SNMP Trap**"
2. Enter hostname or ip address of the recipient. Also, enter SNMP port and community. Default values 162 for port and public for community
3. Click "**Save**"

Note

The SnmpTrapOid will be .1.3.6.1.4.1.2162.100.4.1.2.1
Varbinds will include the display name of the device whose configuration has been changed, its IP address, the type of configuration that underwent change - startup or running and the login name of the user who changed the configuration.
Refer ADVENTNET-DEVICEEXPERT-MIB present under <DeviceExpert Home>/protocol/mibs directory

Generating Trouble Tickets

Upon detecting changes in configuration, you have the option to generate trouble tickets to your Help Desk. To generate trouble tickets,

1. Click the checkbox "**Generate Trouble Tickets**"
2. Enter the Email id of the help desk. By default, the Help Desk id configured through Admin >> Mail Settings page are displayed here. You may add new Email ids if required
3. Provide a subject for the notification and the actual message in the respective fields. Here, in the subject and message fields, you have the option to provide details such as Device Name, IP, type of configuration that underwent change (startup/running), and who changed the configuration
4. For this purpose, DeviceExpert provides replaceable tags - $DEVICENAME, $DEVICEIP, $CONFIGTYPE and $CHANGEDBY. You may use these tags to provide exact details in the subject and message fields of the notification.

   Example: $CONFIGTYPE of $DEVICENAME changed

   Explanation: If the $CONFIGTYPE is "Running Configuration" and $DEVICENAME is "Primary Router", the actual message in the notification would be "Running Configuration of Primary Router changed". These tags get replaced with the actual values at runtime.
5. You have the option to append the configuration diff in the message. The difference with the previous version would be pasted in the message field. To enable this option, click "Append Configuration Difference in Message". Click "**Save**"

Rollingback Configuration

Upon detecting changes in configuration, you have the option to revert to the previous version or to the baseline version. To revert to a configuration version,

1. Click the checkbox "**Rollback Configuration**"
2. If you want to rollback to the previous version - that is, the version immediately preceding the current version (the changed version), choose "Rollback to previous version". When you choose this option, whenever a configuration change is detected, it will immediately be rolled back to the previous version. For example, if a change is detected in the running configuration of a device, and the new version number (changed one) is 7, it will be automatically rolled back to version 6
3. If you want to rollback to the baseline version - that is, the version labeled as the best one, choose "Rollback to version labeled baseline". When you choose this option, whenever a configuration change is detected, it will immediately be rolled back to the baseline version

Note: The rollback feature is for preventing unauthorized configuration changes. So, when you have enabled this feature for a particular device, even a well intended configuration change will also be rolled back. So, if you want to do a genuine configuration change, you need to disable the change management rule.

Important Note:

1. With the completion of the above step, the rule thus created gets automatically associated with the particular device from whose device details page it was created.
2. By following exactly the same steps as above, rules can be created from Device Groups page. When doing so, the rule will be automatically associated with all the devices of the group.
3. The Change Management rule associated with a device/device group can be disassociated anytime from the "Inventory" >> "All Devices" >> "Change Management" GUI

Associating More Rules with a Device/Group

The rules created as above can be associated with other devices/groups. Also, a single device/group can be associated with multiple rules.

To associate a single device with a rule/rules,

1. Go to **"Inventory" >> "All Devices"** and click the hostname of any of the device
2. Click the tab "**Change Management**"
3. In the "**Change Management**" GUI that opens up, click the button "**Associate Rules**"
4. In the page that opens up, the names of available rules are listed. Select the rule/rules, which are to be associated with the device
5. Click "**Associate**". The rule is associated with the required device

To associate a device group with a rule/rules,

1. Go to the "**Inventory**" >> "**Device Group**". Click the name of the required device group
2. In the page that opens up, go to "**Change Management**" tab and slick "**Associate Rules**"
3. In the page that opens up, the names of available rules are listed
4. Select the rule/rules, which are to be associated with the device group and click "**Associate**". The rule/rules are associated with the device group. The rule applies to all devices that are part of the group.

Important Note:
If a rule is modified, the change takes effect for all the devices/groups associated with it.

Managing Change Management Rules

Disabling, Enabling & Removing a Rule

All the change management rules created in the application can be viewed and managed from the "Admin" tab. You can do actions such as temporarily disabling the execution of a rule, enabling it again later or removing the rule altogether.

To manage rules,

1. Go to "**Admin**" tab. Click the link "**Change Management**" present under the "**Device Management**" section in the LHS
2. Select the rule(s) to be disabled/enabled/removed from the list of rules and click the appropriate button

Warning: When you click "Remove", it removes the rule permanently from the database.

Compliance

Overview

Government and industry regulations require IT organizations conform to some standard practices. To become compliant with the regulations such as SOX, HIPAA, CISP, PCI, Sarbanes-Oxley and others, device configurations should conform to the standards specified. The standards could be anything - ensuring the presence or absence of certain strings, commands or values. DeviceExpert helps in automatically checking for compliance to the rules defined. Reports on policy compliance and violations are generated.

How does compliance check work?

Users can define a set of rules specifying the mandatory requirements - what the configuration should contain and/or what it should not contain. The rules can be grouped and defined as 'Compliance Policy'. Each device or a group of devices can be associated with the required policy or policies. DeviceExpert will scan the configuration for compliance to the policy defined and report violations.

How does compliance check benefit me?

Compliance check enables network administrators save a lot of time by automating the standards checking process. Besides it helps in

- automating the process of ensuring that every device configuration in the network adheres to important security policies and best practices
- ensuring that the configuration confirms to standard practices to satisfy Government and industry regulations
- simplifying the requirements for standards compliance audit through comprehensive and intuitive reports

How do I enable compliance check?

Enabling compliance check starts with compliance policy creation, which is a three-step process:

1. Add a Rule

Define the line or lines that are to be either compulsorily present or should not be present in the configuration file. A typical example for a rule is checking the access list configuration or checking the community string. Decide what amounts to violation - presence or absence of a particular line or a set of lines in the configuration file

To add a rule,

1. Go to **Compliance** >> **Rule** >> **New Rule**
2. Enter Rule Name, Description and other details
3. Select '**Simple Criteria**' if your requirement is just to check for the presence or absence of a single line or a group of lines in the configuration file

4. If you want to specify more complex criteria using Regular Expression, select '**Advanced Criteria**' and then enter the line in the text field

Simple Criteria

Criteria	Description	Example
Should contain all lines	The configuration to be checked for compliance should contain all the lines specified by you. Even if a single line is not found, it will be pronounced as 'violation'. DeviceExpert goes about checking the lines (specified by you) one-by-one against the configuration file. It is not necessary that the lines should be present exactly in the same order as specified by you. Since the check is done line-by-line, it is enough if the all the lines are present anywhere in the configuration.	**Criteria**: Should contain all lines **Configuration lines to check**: snmp-server community public RO snmp-server community private RW snmp-server community public1 RO snmp-server community private1 RW **Violation:** If any or all the lines are NOT present in the configuration file (irrespective of the order of the presence of the lines)
Should not contain any line	Exactly opposite to the above. The configuration to be checked for compliance should NOT contain any of the lines specified by you. Even if a single line is found, it will be pronounced as 'violation'. DeviceExpert goes about checking the lines (specified by you) one-by-one against the configuration file. The order of the lines are not important.	**Criteria**: Should not contain any line **Configuration lines to check**: snmp-server community public RO snmp-server community private RW snmp-server community public1 RO snmp-server community private1 RW **Violation:** If any or all the lines are present in the configuration file (irrespective of the order of the presence of the lines)
Should contain exact set	This is similar to 'Should contain all lines', but the difference is that the order of the lines is taken into consideration. If you have specified four lines, DeviceExpert will go about checking if all the four lines are present in the same order as specified. If the lines are not present exactly as specified, it will be pronounced as rule violation.	**Criteria**: Should contain exact set **Configuration lines to check**: snmp-server enable traps hsrp snmp-server enable traps config snmp-server enable traps entity snmp-server enable traps envmon **Violation:** If all the lines are NOT present in the configuration file in the same order (and same set) as specified

Criteria	Description	Example
Should not contain exact set	Exactly opposite to the above. This is similar to 'Should not contain any line', but the difference is that the order of the lines is taken into consideration. If you have specified four lines, DeviceExpert will go about checking if the configuration contains the all the four lines in the same order as specified. If the lines are present exactly as specified, it will be pronounced as rule violation.	**Criteria**: Should not contain exact set **Configuration lines to check**: snmp-server enable traps hsrp snmp-server enable traps config snmp-server enable traps entity snmp-server enable traps envmon **Violation:** If all the lines are present in the configuration file in the same order (and same set) as specified

Advanced Criteria
You can make use of certain Regular Expressions in providing the criteria for checking the configuration for compliance. The following are few examples:

Regular Expression Patterns & Description

Matching specific characters
Characters inside square brackets can be used to match any of the characters mentioned therein.
Example:
[abc] - This is to look for any of the characters a, b or c. The matching is case-sensitive.

Matching a range of characters or numbers
Character range inside square brackets can be used to match any of the characters in the range specified therein. The character range could be alphabets or numbers. The matching is case-sensitive.
Examples:
[a-zA-Z] - This will match any character a through z or A through Z
[0-9] - This will match any digit from 0 to 9

Other Specific Matches

. a dot can be used to match any single character, including space.
\d to match any digit from 0 to 9
\D to match any character other than a digit (0-9)
\s to match a single space character
\S to match any character other than space
X? question mark preceded by a character. The character (in the example here 'X') that precedes the question mark can appear at the most once or does not appear at all
X* asterisk preceded by a character. The character (in the example here 'X') can appear any number of times or not at all
X+ plus sign preceded by a character. The character (in the example here 'X') must appear at least once
X|Y characters separated by a pipe symbol. This is to match either first character or the next one. In the example here, this is to match either X or Y

For more details, refer to the "Regular Expression Tutorials" of Java Tutorials.
More Examples:

Description	RegEx Pattern
To check if there is a 'public' community present in the configuration	**snmp-server community public RO|RW** - to match any line containing the text "snmp-server community public" followed by either "RO" or "RW"
To check if logging to a syslog server has been configured	**logging \S+** - to match any line containing the text "logging" followed by an ip address
To check if enable secret is configured	**enable secret \d \S+** - to match any line containing the text "enable secret" followed by any single digit from 0 to 9 AND any character other than space appearing at least once

Criteria	Description	Example
Should contain	The configuration to be checked for compliance should contain the line matching the RegEx pattern specified by you.	**Criteria:** Should contain line(s) as per the RegEx pattern defined **Configuration lines to check:** snmp-server community public RO|RW **Violation:** If the line "snmp-server community public" followed by either "RO" or "RW" is NOT present
Should not contain	The configuration to be checked for compliance should not contain the line matching the RegEx pattern specified by you.	**Criteria:** Should not contain line(s) as per the RegEx pattern defined **Configuration lines to check:** snmp-server community public RO|RW **Violation:** If the line "snmp-server community public" followed by either "RO" or "RW" is present
Usage of AND/OR condition	Two or more RegEx patterns defined for 'Should Contain' or 'Should not contain' could be combined through AND/OR conditions	--

Finally, specify the **severity** for violation. Click "**Save**".

2. Group the Rules

You can create many rules to cater to specific requirements. A 'Rule Group' refers to a collection of rules. Create a 'Rule Group' by selecting the required rules.

To create a rule group,

1. Go to **Compliance** >> **Rule Group** >> **New Rule Group**. Enter Rule Group Name, Description and other details
2. Select the rule/rules to be added to this group. Click "Save".

3. Create Policy

Once a rule group is created, you can go ahead to create the required compliance policy by selecting the required Rule Groups. Compliance check is done on all policies associated with a device.

To create a policy,

1. Go to **Compliance** tab >> **Policy** >> **New Policy.** Enter Policy Name, Description and other details
2. Specify the configuration file type (running/startup) against which the rules in this policy should be checked. For example, if you choose 'Running' only the current running configuration of the device will be checked for compliance with this policy
3. Select the 'Policy Violation Criteria' - i.e specify what amounts to policy violation - your policy might contain different rules with different severities; you can specify here as violation
    - if any rule (irrespective of the severity is found violated) (OR)
    - only crtical or major rules are violated
4. Select the required rule groups and click 'Save'

4. Associate Devices with Compliance Policy

After creating a policy, you need to associate it with the required devices/device groups.
To associate a policy with a device/devices,

1. Go to **Compliance** tab >> **Policy**. Click the link '**Associate**' present against the policy
2. Select the devices / device groups and click '**Save**'

Running Compliance Check

After associating a policy with a device or device group, you are ready to run compliance check.

To run compliance check for a single device,

1. Go to **"Device Details"** page of the specific device and click the tab **"Compliance"**
2. Click "**Run Compliance Check**" present under the box "**Compliance Actions**". You can even add a schedule for compliance check to be executed at a future point of time. To schedule this, click "**Schedule Compliance Check**" and fill in the details. When you schedule compliance check, you get the option to notify policy violations to desired recipients by email

To view the result & generate compliance report,

1. Compliance status of a specific device will be displayed in the same page. If the device is associated with more than one policy, the compliance check result for each policy is displayed in the table.
2. You can generate a consolidated report of compliance check result for the device. The report provides the compliance result for all the policies associated with the device as a single report. The report can be generated as a PDF/CSV and it can even be emailed to desired recipients

To run compliance check for a device group,

1. Go to **"Inventory" >> "Device Group"** page and click device group for which compliance check has to be run
2. Click the tab **"Compliance"**
3. Click "**Run Compliance Check**" present under the box "**Compliance Actions**". You can even add a schedule for compliance check to be executed at a future point of time. To schedule this, click "**Schedule Compliance Check**" and fill in the details. When you schedule compliance check, you get the option to notify policy violations to desired recipients by email

To view the result & generate compliance report,

1. Compliance status of the selected device group will be displayed in the same page. The compliance result for each device which forms part of the group is displayed in the table. If the device group is associated with more than one policy, the compliance check result for each policy is displayed in the table.
2. You can generate a consolidated report of compliance check result for the device group. The report provides the compliance status and violation details for every device in the device group. The report can be generated as a PDF/CSV and it can even be emailed to desired recipients

Running Adhoc Tests

During any stage of compliance policy creation (rule creation, rule group creation & policy creation), you can perform checks on adhoc basis to test the validity of the rule/rule group/policy added by you. The adhoc tests depict the results then and there. After adding a rule, you can perform adhoc test for a device/device group by clicking the "**Adhoc Test**" button present in **Compliance >> Rule** GUI. Similarly, adhoc tests can be performed for rule group from **Compliance >> Rule Group** GUI and for Policy from **Compliance >> Policy** GUI.

Role-based User Access Control

Contents

Overview

DeviceExpert deals with the sensitive configuration files of devices and in a multi-member work environment, it becomes necessary to restrict access to sensitive information. Fine-grained access restrictions are critical for the secure usage of the product. Therfore a role-based access control to achieve this. It imports the users and their roles from OpManager.

Access levels:

Access Level (Role)	Definition
Administrator	With all privileges to access, edit and push configuration of all devices. Only administrator can add devices to the inventory, add users, assign roles and assign devices. In addition, administrator can approve or reject requests pertaining to configuration upload (pushing configuration) by operators.
Operator	With privileges to access and edit configuration of specified devices. Can send requests for configuration upload (pushing configuration) to Administrators.

This section explains how to create users and assign roles for them.

User Management

User Management Operations such as adding new users and assigning them roles, editing the existing users and deleting the user could be performed only by the Administrators from OpManager. Other types of users do not have this privilege.

Administrators can create as many users as required and define appropriate roles for the user. In DeviceExpert, from Administrator login you can view only the list of existing users.

To view the existing list of users

From DeviceExpert, go to **Admin >> General Settings >> User Management.** The list of users will be displayed with respective login names, access levels and email IDs

Adding New Users

You can add new users from OpManager.

To modify the Email-id of existing Users

1. Go to **Admin >> General Settings >> User Management**
2. In the UI that opens, click the edit icon present against the respective username
3. Change the Email-id and Click "Update"

Privileges for Configuration and other Operations

The following table explains the privileges associated with each access level for performing various device configuration operations:

Access Level	Configuration & Other Operations					
	Device Addition	**Upload (Pushing configuration into the device)**	**Authority for approving various requests**	**Compliance**	**Admin Operations**	**User Management**
Administrator	✓	✓	✓	✓ (create, associate compliance policies)	✓	✓
Operator	✗	✓ (only for authorized devices, subject to approval by administrator)	✗	✗	✗	✗

Approving Configuration Upload Requests

Only Administrators have the absolute privilege to perform all configuration operations. Other users in the hierarchy have restricted privileges.

Any operation that involves pushing configuration into the device (upload) requires the approval of Administrators. When operators perform any such upload operation, a request is filed for the approval by the Administrators. Email notification regarding the request is also sent to the designated Administrators. The request would be evaluated by the Administrators and they have the privilege to approve or reject the request. If the request is approved, the upload operation requested by the user gets executed.

To approve/reject a request,

Go to **"Admin" >> "Device Management" >> "Upload Requests"**
Click "**Pending requests**". The list of all requests pending for approval are listed. Details such as the type of request, name of the user who made the request and requested time are all listed

- Upon clicking a request, all details pertaining to that particular request are listed. You can view the proposed configuration change. Click "Approve" or "Reject" after providing your comment for the decision

[Operators can view the status of their request by following the above procedure].

Note:

1. When Administrators approve a upload that is scheduled to be executed at periodic intervals, the following will be the behaviour:

   Once approved, the upload schedule will not be sent for re-approval during the subsequent executions. For example, consider that a schedule has been created by an operator to upload configuration at a periodic interval of one hour. In this case, the schedule would be submitted for approval only once. If the administrator approves it, it will get executed every hour. From the second schedule onwards, it will not be sent for approval each time.

2. In case, the Administrator rejects an upload request based on a Schedule, the respective request will be deleted from the database.

Automation Using Templates & Scripts

Overview

Quite often, there arises a need to carry out changes to the running configuration of devices and at times, same set of changes need to be applied to multiple devices. Though network administrators can very well edit the configuration manually, the task can prove to be arduous due to the volume of changes and the repetitive nature of the work. DeviceExpert provides a simple solution for this by way of 'Configuration Templates', 'Scripts' and 'Advanced Scripts'.

What are benefits of Custom Templates & Scripts?

- The templates help in automating repetitive and time-consuming configuration tasks. All that you need to do is to create a small template containing the required commands and then execute the template for carrying out repetitive tasks for many devices, many times.
- The templates can also be scheduled for execution at a any point of time in future. This helps in executing the tasks without the intervention of the administrators
- Templates are very helpful for carrying out a partial configuration change to devices at one go.
- The templates enable the network administrator to apply the changes to multiple devices at one go. Also, the templates provide the benefit of carrying out exact changes with precision

How do Custom Templates & Scripts Work?

As the name itself implies, Custom Templates are the ones defined and created by the users themselves in accordance with their needs. A custom template contains the commands (provided by the user) to be executed on the device. A custom template can be created to configure any feature on a device. For instance, you can create a template to configure IGRP on a cisco router. The real power of a custom template lies in reusing the template across multiple devices for bulk configuration updates. For example, a single template could be used for changing the passwords of multiple devices many times. Similarly, a template for firmware upgrade could be used many times for many devices.

To enhance the reusability of a template, 'Template Variables' are defined. A template variable is a placeholder for a value. It can be specified when the template is uploaded to the device. After creating the template, when you wish to upload the changes to a particular device or a number of devices, you just need to provide the values for the template variables. Everything else is automatically taken care of by DeviceExpert.

Note: Creating 'Template Variables' is optional. You may create template variables if you want to enhance the reusability of the template.

Types of Custom Templates in DeviceExpert

Custom templates offered by DeviceExpert are of two types:

1. **TFTP Mode** - for uploading a partial configuration change to a device/devices through TFTP.
2. **Script Execution Mode** - commands are executed on the CLI console one after another. Script execution is divided further into two types as below -
   - Simple Script Execution
   - Advanced Script Execution

The following table provides information about the each type of custom template and when to use them:

TFTP Mode	Simple Script Execution	Advanced Script Execution

TFTP mode is for uploading a partial configuration change to a device/devices through TFTP.
Example:
Enabling TELNET service
Changing SNMP Community
Forwarding Syslog messages
Changing the interface
In all the above case, TFTP mode of configuration upload could be used. In general, for carrying out changes to existing configuration, this mode could be used.
For other cases like executing a command on device, Script execution mode has to be used.
	To execute a single command on the CLI console.
	Example: Synchronizing Running & Startup Configurations. Through a single line in the script containing the command *copy running-config startup-config*, you can synchronize the startup and running configurations of any number of devices.
	Other Examples:
	Changing Passwords
	Updating NTP Server Entries
	Getting 'show version' output
		To execute a series of inter-connected commands on a device in command line. After the execution of one command, some input has to be provided before the next command is invoked. In such a situation, advanced scripting would be useful.
		
		When the execution of a command changes the prompt of the device or takes too much of time to execute or requires fine-grained control to track the flow, advanced script execution has to be used.
		
		Example: Backing up your current IOS image to a TFTP server. To do this, the following sequence would be used:
		Command to be used **copy flash <filename> tftp**
		<filename> - the location of your current IOS image
		TFTP server's IP has to be specified
		The file where it has to be copied, has to be specified
		
		The above sequence of command execution could be transformed into an advanced script as below: (for details on advanced script, click here)
		
		`<command prompt=']?'>copy flash:/%SOURCE_FILE_NAME% tftp</command>`
		`<command prompt=']?'>%TFTP_SERVER_IP%</command>`
		`<command timeout='70'>%DESTINATION_FILE_NAME%</command>`
		
		Other Examples:
		Uploading OS images / firmware upgrade
		• Configuring banner message
		• Resetting passwords of HP ProCurve and Exteme Summit devices
		• Deleting files from flash

Creating Custom Templates

To Create Custom Templates,

1. Go to **"Admin" >> "Device Management" >> "Custom Templates"** and click **"New Template"**
2. In the UI that opens, provide a name for the template in the text field for 'Name'. In the text field for 'Description', provide details about the new template (for easy reference in future)
3. Select the mode in which you wish to upload the configuration to the device. You can select any of the three modes - TFTP or command line mode or Advanced Script Execution mode. In TFTP mode, the file transfer will take place through TFTP. In the case of command line mode, the commands entered would act as scripts and would be executed in command line mode. You can view the output of the execution and generate the output as PDF too. While the file transfer via TFTP is restricted to the normal configuration update, command line script execution is much powerful, in the sense that it can execute commands in privileged modes such as configure terminal mode. The 'Advanced Script Execution Mode' is still more powerful as it provides the option to execute a series of inter connected commands on a device in command line. **(See below for guidelines on creating advanced scripts)**.
4. In the text field '**Template Content**', enter the configuration commands that are to be uploaded to the device. While entering the configuration command, use %<variable_name>% to create a Template Variable. For instance: snmp-server community **%COMMUNITY% RO**
5. The value for the '**Template Variable**' can be specified when the template is uploaded to the device
6. Click '**Save**'. The new template is added to the list of templates

Guidelines for 'Advanced Script Execution Mode'

As stated above, the 'Advanced Script Execution Mode' is still more powerful as it provides the option to execute a series of inter-connected commands on a device in command line. To enable this, the commands to be executed are to be entered in specific format as detailed below:

Purpose	Syntax
Entering the commands to be executed in the command line	<command>**xyz**</command> **Example:** <command>**copy startup-config tftp**</command>
Specifying the prompt that should appear after executing a command. This can be used in the scripts for firmware upgrade, OS image backup etc.	<command **prompt=']?'**>xyz</command> **Example:** <command **prompt=']?'**>copy startup-config tftp</command> (Here, the prompt ? is placed within single quotes and following a closing square bracket) **Note:** If prompt is not given, default prompt will be used
After executing a command, if you wish the application to wait for a few seconds, you can specify the time	<command **timeout='70'**>copy startup-config tftp</command> **Example:** <command **timeout='70'**>copy startup-config tftp</command> **Note:** Default timeout is 30 seconds

Purpose	Syntax
limit in seconds. This can be used in the scripts for firmware upgrade, OS image backup etc.	
After providing a response to query while executing a command, if the device does not expect the user to press "ENTER" after providing the response, this syntax has to be used <>For example, when the device expects a response (say) 'Y' or 'N' alone and NOT an "ENTER" after that, this syntax has to be used. This can be used in the scripts for firmware upgrade, OS image backup etc.	<command **suffix='$NO_ENTER'**>y</command> **Note:** Default value for suffix is "ENTER", that is, new line
Specifying the prompt that should appear after executing a command. This can be used in the scripts for firmware upgrade, OS image backup etc.	<command **prompt='confirm'**>xyz</command> **Example:** <command **prompt='confirm'**>%DESTINATION_FILE_NAME%</command>

Purpose	Syntax
<>When the command sequence does not expect a response after the execution of a command, this syntax has to be used. This has to used coupled with a timeout value for waiting for sometime in between. **Example:** This can be used for setting banner messages in Cisco devices	<command **prompt='$NO_RESPONSE' timeout='5'**>banner %DELIMITING_CHAR%</command> **Example:** <command **prompt='$NO_RESPONSE'** timeout='5'>banner %DELIMITING_CHAR%</command>

To apply changes using templates

1. The list of all templates created by various users, are listed in the '**Custom Templates'** page (Admin >> Device Management >> Custom Templates) along with other information such as who created the templates, description and timestamp of last modification.
2. If the mode of execution chosen by you is TFTP, you will see the link '**Upload**' under the column "Action". If the mode of execution is "Command Line" or "Advanced Script Execution", you will see the link "**Execute**"

To upload the template to device ,

1. Go to **"Admin" >> "Device Management" >> "Custom Templates"** and click the 'Upload' link present under the "**Action**" column corresponding to the template
2. In the UI that opens, you will see the list of '**Template Variables**', if a variable has been created/defined in the template. Enter the desired value for the respective template variables. For example, for '%COMMUNITY%', you can provide 'public' as the value. After entering the values(s), you can preview the actual configuration with full configuration commands and value for community variable(s). To preview the configuration, click '**Preview**'
3. To apply changes only to specific devices, click the radio button '**Select Specific Device'**. The list of devices are also listed in a box. You can choose any number of devices from that list. [To apply changes to a group of devices, click '**Select Device Group**'. You can select the desired group in the drop-down. If you choose this option, the template would be uploaded to all the devices of the selected group]
4. By default, DeviceExpert triggers configuration backup before and after the execution of the custom temple. You have the option to enable/disable the configuration backup on need basis. In certain cases like firmware upgrade, after the execution of the command, device will go out of network briefly. In such a situation, DeviceExpert will not be able to trigger configuration backup. The custom template execution will also fail. To avoid this kind of scenario, you can disable configuration backup while creating the custom template

5. Click '**Upload**' (for TFTP mode) '**Execute**' (Scrip execution/advanced script execution mode). the configuration as defined in the template will be uploaded to the selected devices

Note:
(1) Command line script execution is not supported for the devices with the protocol 'SNMP-TFTP'

(2) The execution output of custom templates would be visible only to the users who executed the template. That means, users with the role 'Operator' will be able to view the output of the custom templates that are executed by them. They will not be able to view the output of the templates executed by other users. Administrators will be able to view the output all the templates and they will also be able to delete the output.

Practical Applications of Command Line Script Execution

Command line script execution of custom templates would prove to be a powerful tool for various bulk operations on multiple devices. Following are few practical applications of the same.

Changing Passwords

You rotate the passwords on multiple devices at one go using the command line script execution. Following is the typical template content that could be used for this purpose:
configure terminal
enable password xxxx
exit

Getting 'show version' output of all devices

You can even execute various commands to get hardware information from a single device or multiple devices. For example, with just the following command in the script, you get 'show version' output for multiple devices at one go:
show version

Updating NTP server entries on your devices

If you wish to update NTP server details in many details, all that you need to do is to create a template as the one below:
configure terminal
ntp server x.x.x.x
exit

Synchronizing Running & Startup Configurations

Just through a single line in the script, you can synchronize the startup and running configurations of any number of devices.
copy running-config startup-config
or
copy startup-config running-config
The above are just an indicative list to demonstrate how the scripts could be used. You may use it for a lot of other applications. Few more examples are available in our website. Please refer to them.

Some Practical Applications of Advanced Script Execution

Uploading OS images

Uploading of OS images/firmware is one of the commonest operations performed by the administrators. Advanced Script Execution can be used to upload the images. The image files can be transferred via TFTP.

Following will be the sequence of command execution for OS image/firmware upload:

Copy the IOS image to TFTP server
Provide the command for copying the image
Provide TFTP server IP
Provide the source filename to copy the file to flash
Provide the destination filename where it has to be copied

The above sequence of command execution could be transformed into an advanced script as below:

```
command prompt=']?'>copy tftp: flash:</command>
<command prompt=']?'>%TFTP_SERVER_IP%</command>
<command prompt=']?'>%SOURCE_FILE_NAME%</command>
<command prompt='confirm'>%DESTINATION_FILE_NAME%</command>
<command timeout='120' suffix='$NO_ENTER'>y</command>
```

In the above example, placeholders have been used for Source File Name, TFTP Server IP and Destination File Name. At the time of executing this advanced script, values could be provided for these placeholders. The script could be used for many devices at one go.

Backing up your current IOS image to a TFTP server

To backup your current IOS image to a TFTP server, the following sequence would be used:

Command to be used **copy flash <filename> tftp**
<filename> - the location of your current IOS image
TFTP server's IP has to be specified
The file where it has to be copied, has to be specified

The above sequence of command execution could be transformed into an advanced script as below:

```
<command prompt=']?'>copy flash:/%SOURCE_FILE_NAME% tftp</command>
<command prompt=']?'>%TFTP_SERVER_IP%</command>
<command timeout='70'>%DESTINATION_FILE_NAME%</command>
```

In the above example, placeholders have been used for Source File Name, TFTP Server IP and Destination File Name. At the time of executing this advanced script, values could be provided for these placeholders. The script could be used for many devices at one go.

Configuring Banner Message

You can edit an existing banner message of a device or a group of devices using the advanced script execution. Users will be presented with this banner every time they attempt a connection with the device.

Normally, the desired banner message is entered within two delimiting characters. For example, within # and #. All the content between these two characters will appear as banner message. The delimiter will not be part of the banner message.

Following will be the sequence of command execution for configuring banner message:

- Enter into the configure terminal mode
- Provide the command for configuring the banner message
- Provide the delimiting character
- Provide the banner message
- Specify the end of the message through the delimiting character again

The above sequence of command execution could be transformed into an advanced script as below:

```
<command>conf t</command>
<command prompt='$NO_RESPONSE' timeout='5'>banner %DELIMITING_CHAR%</command>
<command prompt='$NO_RESPONSE' timeout='5'>%BANNER_LINE_1%</command>
<command prompt='$NO_RESPONSE' timeout='5'>%BANNER_LINE_2%</command>
<command>%DELIMITING_CHAR%</command>
<command>end</command>
```

In the above example, placeholders have been used for Delimiting Character and Banner Message. At the time of executing this advanced script, values could be provided for these placeholders. The script could be used for many devices at one go.

Resetting the Passwords of HP ProCurve Devices

Using the 'Advanced Script Execution' mode, you can reset the passwords of HP ProCurve devices.

Following will be the sequence of command execution for resetting the password:

- Enter into the configure terminal mode
- Provide the command for resetting the password
- Enter the new password
- Confirm the new password

The above sequence of command execution could be transformed into an advanced script as below:

```
<command>conf t</command>
<command prompt='$NO_RESPONSE' timeout='5'>password manager</command>
<command prompt='$NO_RESPONSE' timeout='5'>%PASSWORD%</command>
<command prompt='$NO_RESPONSE' timeout='5'>%PASSWORD%</command>
<command>end</command>
```

In the above example, placeholders have been used for entering and confirming the new password. At the time of executing this advanced script, values could be provided for these placeholders. The script could be used for many devices at one go.

Deleting a file from flash

Cisco IOS images are stored in Flash memory. So, when you to install a new IOS image, you need to make sure your device has enough flash memory to support the image. In case, the device is running short of memory, you will have to delete the files from flash. This can be achieved using an advanced script.

Following will be the sequence of command execution:

- Command to be used **delete flash <filename>**
  <filename> - name of the file to be deleted
- The sequence will seek a confirmation for deletion. <filename> to be entered as a mark of confirmation
- The confirmation should NOT be followed by "ENTER"

The above sequence of command execution could be transformed into an advanced script as below:

```
<command prompt=']?'>delete flash:/%FILE_NAME%</command>
<command prompt='confirm'>%FILE_NAME%</command>
<command suffix='$NO_ENTER'>y</command>
```

In the above example, placeholder has been used for the name of the file to be deleted. At the time of executing this advanced script, value could be provided for this placeholder. The script could be used for many devices at one go.

Scheduling Custom Templates

All the three types of custom templates - TFTP mode, script execution mode and advanced scripts could be scheduled for execution at a future point of time. Refer to the section under schedules for more details.

Managing Templates & Scripts

To view/edit a custom template,

If you to view the contents of an already created template or you want to edit the template,

1. Go to **"Admin" >> "Device Management" >> "Custom Templates"** and click the name of the custom template to be viewed
2. In the UI that opens, click 'Edit Template' and carry out the desired change and click 'Update'

To remove a custom template,

1. Go to **"Admin" >> "Device Management" >> "Custom Templates"** and select the template(s) to be removed
2. Click "**Remove Template**". The template would be removed permanently

Audit

Contents

Overview

Users perform various operations on device configuration such as backing up the configuration, uploading configuration to device, enabling real-time change detection etc., To ensure security aspects, it is essential to record the information on who invoked what operation, on what device, at what time and the result of the operation. This is done by the Audit module of DeviceExpert and this is termed as "Device Operation Audit".

Besides, information about the various scheduled tasks executed by DeviceExpert along with details such as schedule name, result of execution etc., are listed by the Audit Module under "Schedule Audit".

Viewing Operation Audit Details

As stated above, Operation Audit provides the following information:

1. Operation Name & Status (Backup, Upload, Enabling Configuration Change Detection, SNMP Configuration etc.,)
2. Invoked by whom - by SYSTEM or by a USER
3. Time of Execution and
4. Detailed message about the outcome of operation. In case of operation failure, the reason for the failure.

To View Operation Audit Details,

1. Go to "Inventory" and click the icon depicting "**Actions**" and click "**Device Audit**"
2. operation audit details would be listed in the UI

Alternatively, to view the audit records pertaining to a specific device, you can use the "**Device Operation Audit Report**" link in the **Device Details >> Reports** page. This will show the audit records of a specific device.

The Audit Details page gets refreshed every five minutes.

To filter the Audit Trails view,

You can restrict the view page of audit trails to view only the trails pertaining to a device group and/or the trails that were generated over a fixed time range - say Today, Yesterday, Last seven days, Last thirty days and a custom period. By default, audit trails pertaining to all device groups recorded today gets listed. You can filter and view the details in accordance with your needs. You can filter the trails by selecting the desired "Device Group" from the drop-down and the desired "Time Duration" from the icon available in the UI.

Viewing Schedule Audit Details

Refer to the section "Schedules"

Adding Schedules

Contents

Overview

If you have a large number of devices, carrying out operations such as backup, upload etc., become monotonous, if they are to be done manually. You might also require to perform certain operations at regular intervals. Execution of these operations can be automated - that is they can be scheduled for execution at the required time automatically.

Tasks such as

1. Configuration Backup
2. Report Generation and
3. Compliance Check
4. Custom Templates

for a specific device or group of devices could be scheduled for execution at a future point of time. These tasks can be scheduled for automatic execution at periodic intervals or for an one-time execution.

Adding Schedules

Periodic Configuration Backup

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. In the UI that opens, click **"New Schedule"**
3. In the UI that pops-up, provide a name for this schedule in the textfield for the parameter **"Schedule Name"**
4. Choose **"Configuration Backup"** in the drop-down for **"Task type"**
5. Specify the required recurrence option
6. Select the devices that are to be backedup. You can either choose a list of **"Specific Devices"** or a **"Device Group"** [if you choose a device group, all the devices in the group will be backedup]
7. The result of the scheduled task could be sent as an email notification to any number of users. Just add the email IDs to the "**Recipient list**" and select the recipients to whom notifications are to be sent. Sending notifications is optional. Finally, click **"Save"**

Periodic Report Generation

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. In the UI that opens, click **"New Schedule"**
3. In the UI that pops-up, provide a name for this schedule in the textfield for the parameter **"Schedule Name"**
4. Choose **"Report Generation"** in the drop-down for **"Task type"**

5. Select the required report from the drop-down for "**Report Type**"
6. Specify the required recurrence option
7. Select the devices for which the report is to be generated. You can either choose a list of **"Specific Devices"** or a **"Device Group"** [if you choose a device group, the report will be generated for all the devices in the group]
8. The result of the scheduled task could be sent as an email notification to any number of users. Just add the email IDs to the "**Recipient list**" and select the recipients to whom notifications are to be sent. Sending notifications is optional. Finally, click **"Save"**

Scheduled task for Compliance Check

Prerequisite:

Before adding a schedule for compliance check, compliance policy should have been associated with the devices. Refer to the section on Compliance Policies for more details.

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. In the UI that opens, click **"New Schedule"**
3. In the UI that pops-up, provide a name for this schedule in the textfield for the parameter **"Schedule Name"**
4. Choose **"Compliance Check"** in the drop-down for **"Task type"**
5. Specify the required recurrence option
6. Select the devices whose configuration has to be checked for compliance. You can either choose a list of **"Specific Devices"** or a **"Device Group"** [if you choose a device group, compliance check will be run for all the devices in the group]
7. The result of the scheduled task could be sent as an email notification to any number of users. Just add the email IDs to the "Recipient list" and select the recipients to whom notifications are to be sent. Sending notifications is optional. Finally, click **"Save"**

Scheduled Task for Custom Templates

All the three types of custom templates - TFTP mode, script execution mode and advanced scripts could be scheduled for execution at a future point of time:

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. In the UI that opens, click **"New Schedule"**
3. In the UI that pops-up, provide a name for this schedule in the textfield for the parameter **"Schedule Name"**
4. Choose **"Custom Template"** in the drop-down for **"Task type"**
5. Select the required template from the drop-down for "**Choose Custom Template**"
6. Provide the values for the template variable
7. Specify the required recurrence option
8. Select the devices on which the template has to be executed. You can either choose a list of **"Specific Devices"** or a **"Device Group"** [if you choose a device group, the template will be executed on all the devices in the group]
9. The result of the scheduled task could be sent as an email notification to any number of users. Just add the email IDs to the "**Recipient list**" and select the recipients to whom notifications are to be sent. Sending notifications is optional. Finally, click **"Save"**

Audit of Scheduled Task Execution

Tasks that were executed for a particular schedule (from the time of creation of the schedule up to the current time) can be viewed as a snapshot. This history provides starting time of the schedules, their ending time and also the result of execution.

To view the Audit of Schedule task execution,

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. In the UI that opens, click the link **"View"** in Audit column of each schedule

Audit can also be viewed from the "Device Details" page of the respective devices.

Managing Schedules

The scheduled tasks once created, can be managed from the "All Schedules" UI from where you can

1. view the properties of scheduled tasks
2. edit the scheduled tasks
3. remove the schedules

Viewing the Properties of Scheduled Tasks

To view the properties of scheduled tasks,

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. Click the name of the schedule whose properties are to be viewed

Editing Schedules

To view edit the properties of scheduled tasks,

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. Click the name of the schedule whose properties are to be edited
3. Edit the details and click "**Save**"

Enabling/Disabling Schedule

At times, you would require to temporarily stop the execution of a scheduled task and would like to resume it again at some other point of time.

To disable a schedule,

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. Select the name of the schedule which is to be disabled and click "**Disable**"

To enable the schedule,

click "**Enable**"

Removing a Schedule

If a scheduled task is not needed, you can remove it from the list of schedules.

To remove a schedule,

1. Go to **"Admin" >> "Device Management" >> "All Schedules"**
2. Select the name of the schedule which is to be disabled and click "**Disable**"
3. Click "**Remove**"

Reports

Contents

Overview

The information on the entire network configuration management process in your enterprise is presented in the form of comprehensive reports in DeviceExpert. The status and summaries of the different activities such as device configuration details, changes in configuration, network inventory, conflict between startup and running configuration, device audit details, policy compliance details etc are provided in the form of tables and graphs, which assist the network administrators to make a well-informed decisions on device configuration.

Types of Reports

DeviceExpert provides over 12 reports under four categories:

1. Network Reports
2. Configuration Reports
3. User Reports
4. Policy Compliance Reports

Network Reports

All details pertaining to the device properties, hardware properties, firmware details, audit details pertaining to the devices etc have been presented under Network Reports.
To access the Network Reports, just go to the "**Reports**" tab.

Report Name	What does it Convey	Additional Information
Hardware Inventory Report	The hardware properties of each device of all available device groups are presented in this report. The report is displayed on 'device group' basis. Click "**Hardware Inventory Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.
Firmware Inventory Report	The OS details of devices such as OS type, version (of each device of all available device groups) are presented in this report. The report is displayed on 'device group' basis. Click "**Firmware Inventory Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.

Report Name	What does it Convey	Additional Information
Device Inventory Report	Details such as the model number, series, type etc of each device of all available device groups are presented in this report. The report is displayed on 'device group' basis. Click "**Device Inventory Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.
Network Health Status Report	Details such as the status of configuration backup, information if the startup and running configurations differ, information on policy compliance etc of each device of all available device groups are presented in this report. The report is displayed on 'device group' basis. Click "**Network Health Status Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.
Device Management Status Report	Status of basic device management details - if credentials have been supplied, the protocol used (for communication between the device and DeviceExpert), the status of real-time change detection etc of each device of all available device groups are presented in this report. The report is displayed on 'device group' basis. Click "**Device Management Status Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.
Device Audit Report	Details on who invoked, what operation and when on each device of all available device groups are presented in this report. The report is displayed on 'device group' basis. Click "**Device Audit Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.

Configuration Reports

Report Name	What does it Convey	Additional Information
Startup-Running Conflict Report	Devices (of each device group) whose startup and running configurations differ are presented in this report. In addition, there is provision to view the difference between the startup and running configurations. The report is displayed on 'device group' basis. Click "**Startup-Running Conflict Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.

Report Name	What does it Convey	Additional Information
Configuration Changes Report	Devices (of each device group) that have undergone changes in configuration are presented in this report. The report is displayed on 'device group' basis. Click "**Configuration Changes Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.
Configuration Change Trend Report	Details on the number of configuration changes done on the configuration of devices (of all device groups) during a particular time period are captured along with the mode of configuration change - whether the changes were done through DeviceExpert or directly from outside the application are captured. The report is displayed on 'device group' basis. Click "**Configuration Change Trend Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.
Configuration Analysis Report	DeviceExpert leverages **Nipper** for generating the Configuration Analysis Report. Nipper processes the Configuration files and reports on various configuration settings. This report is quite comprehensive - Domain Name Settings, Time Zone Settings, User Accounts and Privileges, Logging, SNMP Settings, Protocols, Interfaces and Access Control Lists - are analyzed and the details are depicted in the report. The report is displayed on 'device group' basis. Click "**Configuration Analysis Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.
Security Audit Report	For this report also, DeviceExpert leverages the **Nipper**. Nipper processes network device configuration files, performs a security audit and outputs a security report with recommendations and a configuration report. This report is also quite comprehensive. The configuration files are analyzed from all possible security angles. The report is displayed on 'device group' basis. Click "**Security Audit Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.

User Reports

Report Name	What does it Convey	Additional Information
User Access Report	Device access authorization details for all users are presented in this report. The list of devices assigned for each user are shown by this report. Click "**User Access Report**" in the "**Reports**" tab to generate the report.	--
Configuration Upload Request Report	The status of configuration upload requests made by the operators and information as to whether the requests are pending or were approved or rejected, are presented in this report. Click "**Configuration Upload Request Report**" in the "**Reports**" tab to generate the report.	--

Policy Compliance Reports

Report Name	What does it Convey	Additional Information
Compliance Report	The result of the compliance policy check done on devices (of each device group) are presented in this report. Number of devices that are compliant, number of devices whose configuration is in violation of the policy, number of compliance policies, rules, the time at which the last compliance check was done etc., are presented in this report.. The report is displayed on 'device group' basis. Click "**Startup-Running Compliance Policy Check Report**" in the "**Reports**" tab to generate the report.	In the report display page, you can view the report for the each group by selecting the respective group name in the '**Device Group**' drop-down on the top of the page.

Admin Operations

Contents

Overview

While configuring DeviceExpert for usage in your network, you can perform certain administrative operations. The operations are classified under three categories

1. Device Management
2. General Settings
3. Tools

This section provides information on all the operations classified under the above categories.

Device Management

The following eight operations have been classified as 'Device Management' Operations

1. Custom Templates
2. All Schedules
3. Change Management
4. Credential Profiles
5. Show Commands
6. Upload Requests
7. Label Management
8. Export Configuration

Custom Templates

Refer to the section 'Automation using Templates & Scripts'

All Schedules

Refer to the section 'Scheduling Tasks'

Change Management

Refer to the section 'Configuration Change Management'

Credential Profiles

Refer to the section 'Sharing Common Credentials Across Devices'

Show Commands

Refer to the section 'Viewing Device Configuration Details'

Upload Requests

The list of the configuration upload requests made by the Operators and the status of approval by 'Administrators' or 'Password Administrators' are shown here.

1. Go to **"Admin" >> "Device Management" >> "Upload Requests"**
2. In the UI that opens, the following details are displayed.

Pending Requests - Showing the list of all requests that are pending approval
Approved Requests - Showing the list of all requests that were approved by 'Administrators' or 'Password Administrators'
Rejected Requests - Showing the list of all requests that were rejected by 'Administrators' or 'Password Administrators' along with the reason for rejection

Label Management

For any version of configuration, you can associate a label - that is, a unique tag. As configuration versions keep on changing, you will have difficulty in remembering the version number of a particular good configuration. To avoid that, you can associate the version with a label for easy identification. You can associate labels directly for the current configuration of any device. Labels can be associated with any other desired version also.

Creating Labels

You can create any number of labels and use them whenever needed - that is, associate them with desired configuration versions.

To create labels,

1. Go to **"Admin" >> "Device Management" >> "Label Management"**
2. In the UI that opens, click "**New Label**". Provide a name for the label and in the textfield for "**Description**" provide details for future reference [to remember and identify the label] and click "**Save**"
3. The new label has been created; the name of the label will be listed in UI; it will be listed in all the drop-downs that are related to associating a label

Labeling current Configuration

The current startup and running configuration of any device or group of devices can be labeled with a unique tag. This labelling comes in handy when you want to revert to that particular configuration version. This tagging would also be useful for reverting to a previous good version in the event of a disaster.

To put a label to a current configuration of a device or a group of devices,

1. Go to "**Inventory**" and select the devices whose current configurations are to be labeled
2. Click the button **"More Actions" >> "Label Current Configuration"**
3. In the UI that opens, you can select a label from the available labels OR you can create a new label. In the text field for "Description" provide details for future reference [to remember and identify the label] and click "Update"

Note: You can label the current configurations of devices belonging to a device group from the **"Inventory" >> "Device Group" >> <Name of the Device Group> >> "More Actions" >> "Label Current Configuration"**.

Putting Labels to desired versions

You can associate labels to any desired configuration version. To associate label for a specific version of a particular device, go to **"Inventory" >> "All Devices" >>** go to the "**Device Details**" page by clicking the name of the device. Click "Current Version" against Startup/Running as required and select the desired configuration version from the drop-down; click "**Associate Label**" and follow the steps detailed above.

Export Configuration

Refer to the section 'Disaster Recovery'

General Settings

The following operations have been classified as 'General Settings':

1. Server Settings
2. Mail Settings
3. Proxy Settings
4. Trouble-Ticket Settings
5. SNMP Trap Settings
6. Database Administration
7. Database Backup
8. Log Level

Server Settings

TFTP Server Setting

DeviceExpert uses TFTP server to transfer the configuration files to-and-fro the devices. In case, DeviceExpert is running in multi-homed machines, you can specify the interface to be used for transferring the configuration files from/to the devices. The interface specified here will be used for transferring (backup, upload) configuration files of all devices in inventory.

To specify a particular interface,

1. Go to **"Admin" >> "General Settings" >> "Server Settings" >> "TFTP Server"**
2. Select the required IP from the drop-down. Click **"Save"**
3. To give effect to this change, you need to restart DeviceExpert server

SCP Server Setting

DeviceExpert provides the option to use SCP to transfer the configuration files to-and-fro the devices. In case, DeviceExpert is running in multi-homed machines, you can specify the interface to be used for transferring the configuration files from/to the devices. The interface specified here will be used for transferring (backup, upload) configuration files of all devices in inventory.

To specify a particular interface,

1. Go to **"Admin" >> "General Settings" >> "Server Settings" >> "SCP Server"**
2. Select the required IP from the drop-down. Click **"Save"**
3. To give effect to this change, you need to restart DeviceExpert server

Syslog Server Setting

By default, DeviceExpert binds its syslog listener to port 514. In case, your machine is multi-homed and if you want to run some other application with a syslog server in the same machine, you can bind the DeviceExpert syslog server to a specific interface leaving the other

interface(s) for use by other application(s).
To specify a particular interface,

1. Go to **"Admin" >> "General Settings" >> "Server Settings" >> "Syslog Server"**
2. Select the required IP from the drop-down. Click "Save"
3. <>To give effect to this change, you need to restart DeviceExpert server

Parallel Job Count

DeviceExpert executes configuration operations such as backup, upload, scheduled task execution, report generation etc as parallel jobs. The number of threads available for such parallel tasks are limited. Depending on the hardware configuration of the machine in which DeviceExpert is running, the number of parallel jobs can be increased.

Hardware Configuration	Number of Parallel Job Counts
1.8 GHz Pentium® processor and up to 1 GB RAM	20 - 30
Dual Processor with more than 4 GB RAM	30 - 100

To specify the number of parallel job counts,

1. Go to **"Admin" >> "General Settings" >> "Server Settings" >> "Parallel Job Count"**
2. Select the required number from the drop-down. Click "Save"
3. To give effect to this change, you need to restart DeviceExpert server

Mail Settings

DeviceExpert sends various notifications to the users (for example, reports) using an SMTP mail server running in your network. This section explains how to specify the SMTP server details and entering email IDs.

To specify SMTP Server details,

1. Go to **"Admin" >> "General Settings" >> "Mail Settings"**
2. Enter SMTP server name in the text field, enter SMTP port and enter username and password, if your SMTP settings require authentication
3. In the text field for '**From**' or '**Sender**' address, specify the email id of the originator of the email; by default, the from address is specified as '**noreply@adventnet.com**'.
4. After configuring the 'Mail Settings', you can test if connection could be established with your server. Click "**Test**". DeviceExpert will attempt to establish connection with your mail server. If the configuration is proper and if DeviceExpert is able to establish a connection, you will see the message "**Mail Server connection established successfully**".
5. Click "**Save**", if you have changed SMTP settings

By default, the SMTP server runs in the port 25. You can specify any other SMTP server also.

Proxy Settings

In your enterprise network setup, you might need to go through a proxy server to access the internet. In such a case, you need to configure the username and password for internet access. This section explains how to carry out proxy configuration.

To configure proxy settings,

1. Go to **"Admin" >> "General Settings" >> "Proxy Settings"** tab

The parameters to be configured are:

- **HTTP Proxy Host**: Host name of the proxy server (eg: proxy-server)
- **HTTP Proxy Port**: Port number at which the server is running (eg: 80)
- **Username** to access the internet
- **Password**

After configuring the 'Proxy Settings', you can test if connection could be established with the proxy server. To test, just click the button "Test" of "Test Mail Server". DeviceExpert will attempt to establish connection with proxy server. If the configuration is proper and if DeviceExpert is able to establish a connection, you will see the message "Success".

Trouble Ticket Settings

Upon detecting changes in configuration, DeviceExpert provides the option to generate trouble tickets to your Help Desk. You can set your Help Desk Email id here.

1. Enter Help Desk Email id and click "**Save**" to give effect to the settings

SNMP Trap Settings

SNMP v2 traps could be sent to a specific host upon detecting a configuration change. Settings could be done for that purpose here.

To send SNMP trap to the desired host (based on the change management condition specified through change management rule),

1. Go to **"Admin" >> "General Settings" >> "SNMP Trap Settings"** tab
2. Enter **hostname** or **ip address** of the recipient. Also, enter **SNMP port** and **community**. Default values 162 for port and **public** for community
3. Click "**Save**"

Database Administration

In typical production environments, DeviceExpert would deal with a huge amount of data related to device configuration. Audit logs on who performed what operation and when, also gets piled up in the database. Over a period of time, it becomes too huge a size. If you want to remove unwanted data, you can do periodic database cleanup.
You can perform two types of cleanup operations:

1. Device Audit cleanup
2. Configuration History Cleanup

To cleanup device audit logs,

1. Go to **"Admin" >> "General Settings" >> "Database Administration"**
2. In the UI that opens up, select the checkbox below '**Device Audit Cleanup**'. The audit logs generated prior to a specified number of days could be deleted. For example, if you choose '10 days', all audit logs older than 10 days will be deleted. Also, at any point of time, the audit logs of the recent 10 days alone would be maintained. You can select the days in the range of 10,20,30,60,90 and 120 from the drop-down
3. Click '**Save**'

Configuration History Cleanup

1. Go to **"Admin" >> "General Settings" >> "Database Administration"**
2. In the UI that opens up, select the checkbox below '**Configuration History Cleanup**'. You can specify the maximum number of configuration versions that are to be kept in the database for each device and each configuration type. For example, if you choose to keep 10 versions in the history, only the most recent 10 versions would be kept in the history. This applies independently for each configuration type - that is, latest 10 versions in startup and 10 versions in running would be kept in the history. You can select the number in the range of 10,20,30,40,50 and 100 from the drop-down
3. Click '**Save**'

Important Note: While removing older versions, as per the number set by you, the following rule would be applied.

While removing the versions, BASELINE version and those versions above it will not be removed.

For example, if you want to keep only the latest 10 configuration versions in the history and if there are say 15 versions at present, DeviceExpert will start removing the versions 1,2,3,4 & 5. While doing so, if, say version 3 has been labelled as BASELINE, DeviceExpert will immediately stop the deletion process. Versions 1 and 2 alone would be removed. All versions from 3 to 15 would be left undisturbed even though you have preferred to keep only 10 versions in the history.

Database Backup

Refer to the section on 'Disaster Recovery'

Log Level

In the event of any issues, DeviceExpert server logs help us in getting to the root of the issue. Printing of log messages can be controlled through the two log levels. This section explains how to set the desired level.

Setting Server Log Level

Printing of log messages can be controlled through the two log levels - DEBUG and INFO. DEBUG level prints all messages and it is useful for debugging purposes. The other level INFO prints some information messages. The default Log Level is 'INFO'.

To modify Log Levels,

1. Go to **"General Settings" >> "General Settings" >> "Log Level"**
2. In the UI that opens, select the desired log level from the drop-down and click "**Save**"

Tools

The following operations have been classified under Tools

1. User Management
2. Database Console
3. SysObjectID Finder

User Management

Refer to the section "Role-based user access control"

Accessing Database

To access the Database,

1. Go to **"Admin" >> "Tools" >> "Database Console"**
2. In the console, enter the query to be executed [only 'select' 'delete' and 'update' queries are supported]

Remember the following when executing a query,

1. Table names and table columns are case-sensitive
2. For SELECT queries, set the row limit between 1 and 500. Default row limit is 10

Warning! You are directly accessing the database at your own risk. Any update or delete operations will result in loss of data.

Finding sysObjectID of Devices

When you require support for new device models in DeviceExpert, the sysObjectID of the new device is needed for supporting discovery of the device. To enable you to find the sysObjectID, DeviceExpert provides the tool **sysObjectID Finder**.

To find the sysObjectID,

1. Go to **"Admin" >> "Tools" >> "SysObjectID Finder"**
2. In the UI that opens, provide the Hostname/IP of the device whose sysObjectID has to be found
3. Enter the snmp Read Community credential for the device
4. Set a 'timeout' value and 'retry count' for the sysObjectID finding operation
5. Click 'Find'.
6. sysObjectID and sysDescr of the device are returned

Disaster Recovery

Contents

Overview

In the rare event of something going wrong with DeviceExpert, it is important to have a backup of device configuration to recover from the disaster. DeviceExpert provides two utilities to achieve this:

1. Backing up the device configuration files
2. Backing up the entire database

Once you have the backup, it is easy to achieve a quick disaster recovery. In the DeviceExpert GUI, tools have been provided to export the configuration files & backing up the database. Besides, scripts have been provided to facilitate backup of configuration files or database when DeviceExpert server is not running.

Backing up Device Configuration Files

Storing Configuration on Secondary Storage Devices

If you need a copy of all the device configuration files in DeviceExpert database and want to store them somewhere, here is an option. Configuration files of all devices in the DeviceExpert database can be exported in text format and stored in a separate directory. **Only administrators shall have the permission to do this operation**. You can even store the configuration files in secondary storage devices such as Memory Cards.
The configuration files could be exported on demand at any point of time or it could be scheduled to be generated at periodic intervals - say daily, weekly or monthly.

To export configuration files immediately on demand,

1. Go to **"Admin" >> "Device Management" >> "Export Configuration"**
2. In the UI that opens up, click 'Export Configurations Now'
3. The result of the execution of this operation will be displayed in the UI that opens up
4. The exported configuration files will get stored under <DeviceExpert_Home>/config_backup directory

To schedule export of configuration files,

1. Go to **"Admin" >> "Device Management" >> "Export Configuration"**
2. In the UI that opens up, select the desired option - Daily, Weekly or Monthly. Also, choose the desired time/day/date accordingly
3. You can even intimate the result of the export operation (whether success/failure) to desired recipients via email. Just enter the required email id in the text field
4. Click **'Save'**
5. The schedule will get executed at the required time. You can view the result of the execution by clicking the link **'View Execution History'** present at the top right hand corner

6. The exported configuration files will get stored under <DeviceExpert_Home>/config_backup directory

Note: To disable the execution, select the 'Never' option.

Exporting Configuration files when DeviceExpert Server is not running

DeviceExpert provides a script, which will generate configuration files of each device in text format and store it under a separate directory.

To take backup of configuration files,

1. Open a command prompt and navigate to <DeviceExpert_Home>/bin directory
2. Execute configbackup.bat (in windows) OR sh configbackup.sh (in Linux)
3. A new directory "**config_backup**" will be created under <DeviceExpert_Home> and the configuration files will be saved under this.
4. The filename will be of the format: **<ResourceName>_<FileType>.txt.** For example, cat2900_Running.txt and cat2900_Startup.txt

You can take a backup of '**config_backup**' directory through your own automated backup mechanism.

Backing up the Database

You can take a backup of the whole DeviceExpert Database and restore the contents in the event of a disaster. You can create schedules for DB backup to be taken in periodic intervals - say daily, weekly or monthly.

To schedule export of configuration files,

1. Go to **"Admin" >> "General Settings" >> "Database Backup"**
2. In the UI that opens up, select the desired option - Daily, Weekly or Monthly. Also, choose the desired time/day/date accordingly
3. Specify the maximum number of backup files that are to be stored. That is, every time when backup scheduled is executed, database is backedup and contents are stored afresh. You can choose the maximum number of backup files to be kept
4. You can even intimate the result of the backup operation (whether success/failure) to desired recipients via email. Just enter the required email id in the text field
5. Click '**Save**'. The schedule will get executed at the required time. You can view the result of the execution by clicking the link '**View Execution History**' present at the top right hand corner
6. By default, the backup files will get stored under <DeviceExpert_Home>/Backup directory. If you want, you can configure the destination directory

Note: To disable the execution, select the 'Never' option.

Taking Backup when DeviceExpert Server is not running

DeviceExpert provides a script, which will take backup of DeviceExpert DB and store it under a separate directory.

1. Open a command prompt and navigate to <DeviceExpert_Home>/bin directory
2. Execute backupDB.bat (in windows) OR sh backupDB.sh (in Linux)
3. A new directory "**Backup**" will be created under <DeviceExpert_Home> and the contents of the DB are saved under this directory
4. The filename of the DB backup contents will be of the format: **<YY-MM-DD>-<TIME>.zip.** For example, 060915-1508.zip (That is, backup created at 15:08 hrs on 15 September 2006)

You can take a backup of 'Backup' directory through your own automated backup mechanism.

To restore the backedup contents,

Before restoring the backedup contents in DeviceExpert, make sure you reinitialize the database.

The restoration process takes the following steps:

1. Open a command prompt and navigate to <DeviceExpert_Home>/bin directory
2. Execute deviceexpert.bat/sh reinit
3. Once reinitializing the DB is completed, execute restoreDB.bat <DB Backup file name> (in windows) OR sh backupDB.sh <DB Backup file name> (in Linux)

NFA Plug-in

About NetFlow Plug-in

The NetFlow Analyzer plug-in offers a complete solution to perform in-depth traffic analysis on your network. NetFlow Analyzer uses the flows (netflow, sflow, jflow etc.) exported by the devices to identify traffic caused by them. NetFlow Analyzer provides you the detailed information on the bandwidth being used by the network and allows you to drill down to specific application, conversation, port, user etc that is consuming more and causing the damage. Futher you can generate detailed reports on the bandwidth patterns and take some capacity planning decisions.

By plugging in NetFlow Analyzer with OpManager you can view the traffic handled by the interfaces in their respective snapshot pages. The added advantage with NetFlow Analyzer plug-in is, the user defined in OpManager can access NetFlow Analyzer. Configuring mail server settings in NetFlow Analyzer is also not necessary if it has been configured in OpManager.

The devices that are NetFlow Analyzer enabled are marked with the NetFlow Analyzer icon in their respective maps. The interfaces that are NetFlow enabled are displayed with the icon under the Interface tab in their respective device snapshot pages.

Installation Platform:

NetFlow Analyzer plug-in supports only Windows installation as of now.

Supported DB:

NetFlow Analyzer pug-in supports only MySQL.

Devices Supported:

Click here to get the list of devices that are supported by NetFlow Analyzer.

Ports Used:

- Web: 8080
- NetFlow Listener Port: 9996
- MySQL: 13306

Features:

- Easy Network Troubleshooting
- NetFlow Reporting
- Network Security
- Application Performance Optimization
- Network Traffic Analysis
- Bandwidth Reporting
- Automating Reports
- Faster Network Troubleshooting
- Department wise bandwidth monitoring

Note: Radius Server is not supported in this NetFlow Analyzer plug-in.

Installing NetFlow Analyzer Plug-in

Click here to download the NetFlow Analyzer plug-in. Follow the procedures given below to install:

1. Download OpManager's NetFlow Analyzer plug-in file to OpManager server.
2. Shutdown OpManager Service.
3. Double click OpManager's NetFlow Analyzer plug-in exe file. (You have to install NetFlow Analyzer plug-in in OpManager server only)
4. Follow the on-screen instructions to complete the installation process.
5. Start the OpManager Service.

Note: You should have OpManager 7205 build or later.

Configuring Flow exports

Devices and Supported Flow exports

The following charts specifiesformation on the various vendors and the flow exports their devices support. Click on the specific device name to know how to configure the corresponding flow export.

Device/Vendor	Supported Flow Export
Cisco	NetFlow
Juniper Devices	cflowd, jFlow
Nortel	IPFIX
Huwaei, 3com,H3C	Netstream
Alcatel-Lucent, Extreme Networks, Foundry Networks, HP, Hitachi, NEC, AlaxalA Networks, Allied Telesis, Comtec Systems, Force10 Networks	*sFlow*

Cisco Devices (NetFlow)

Configuring Cisco Devices

This section offers a brief guide to setting up NetFlow on a Cisco router or switch. For more detailed information, refer the Cisco web site at http://www.cisco.com/go/netflow. It is recommended that only people with experience in configuring Cisco devices follow these steps.

- Cisco devices with NetFlow support
- Configuring an IOS Device
- Configuring a Catalyst 6000 Series Switch
- Configuring a Native IOS Device
- Configuring a Catalyst 4000 Series Switch
- Configuring NetFlow for BGP

Setting the appropriate time on the router

NetFlow Analyzer stamps the flows based on the router time. It is therefore important to ensure that the time on the router is set properly. Netflow Analyer can handle routers from different time zones automatically, provided the correct time is set.

Whenever the time difference between the NetFlow Analyzer Server and the router is above 10 minutes a warning icon will appear in the home page. When this happens, NetFlow Analyzer will stamp the flows based on the system time of the NetFlow Analyzer server.

In case you see this, please ensure the following on the router:

- Check if the correct time is set on your router. You can check this by logging into the router and typing ***show clock***. You can set the clock time using the command ***clock set hh:mm:ss date month year***. [An example : ***clock set 17:00:00 27 March 2008***]
- Check if the time zone and the offset (in Hours and Minutes) for the time zone is set properly (E.g. PST -8 00 for PST or EST -5 00 for EST). You can check this by logging into the router, going into the configure terminal and typing ***show running-config***. You can set the clock time zone and offset using the command ***clock timezone zone hours [minutes]*** (E.g. clock timezone PST -8 00)

To enable NetFlow in an MPLS environment refer Cisco's documentation on MPLS NetFlow

Cisco® NetFlow Device Support

The following charts include information on the various vendors and devices supporting NetFlow version 5 or 7 or 9 data export. Use these charts to determine if your devices are compatible with NetFlow Analyzer.

Cisco Routers

Cisco IOS Software Release Version	Supported Cisco Hardware Platforms
11.1CA, 11.1CC	Cisco 7200 and 7500 series, RSP 7200 series
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series
12.0T, 12.0S	Cisco 1720, 2600, 3600, 4500, 4700, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series, MGX8800RPM series, and BPx8600 series
12.0(3)T, 12.0(3)S	Cisco 1720, 2600, 3600, 4500, 4700, AS5300, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series, MGX8800RPM series, and BPx8650 series
12.0(4)T	Cisco 1400, 1600, 1720, 2500, 2600, 3600, 4500, 4700, AS5300, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series, MGX8800RPM series, and BPx8650 series
12.0(4)XE	Cisco 7100 series
12.0(6)S	Cisco 12000 series

NetFlow is also supported by these devices Cisco 800, 1700, 1800, 2800, 3800, 6500, 7300, 7600, 10000, CRS-1 and these Catalyst series switches: 45xx, 55xx, 6xxx.

 **These devices do not support NetFlow: Cisco 2900, 3500, 3660, 3750.**

Cisco Switches

NetFlow export is also supported on other Cisco switches when using a NetFlow Feature Card (NFFC) or NFFC II and the Route Switch Module (RSM), or Route Switch Feature Card (RSFC). However, check whether version 5 is supported, as most switches export version 7 by default.

NetFlow Version 9 Support

Supported Platforms

The following platforms support NetFlow Version 9 Data Export :

- Cisco 2600 series
- Cisco 3600 series
- Cisco 7100 series
- Cisco 7200 series

- Cisco 7300 series
- Cisco 7400 series
- Cisco 7500 series
- Cisco 12000 series

Other Vendors

Some of the major vendors supporting NetFlow include:

- **3Com** - 8800 Series Switches
- **Adtran** - NetVanta 3200, 3305, 4305, 5305, 1524, 1624, 3430, 3448, 3130, 340, and 344. (Supports NetFlow version 9)
- **Juniper Networks** - Does not support sampling interval attribute. First and last times are stored in seconds rather than milliseconds
- **Riverbed**
- **Enterasys Networks**
- **Extreme Networks** - Does not support input/output interface, octets, or first and last times
- **Foundry Networks**

Configuring NetFlow Export on an IOS Device

Follow the steps below to configure NetFlow export on a Cisco IOS device.

Refer the Cisco Version Matrix for information on Cisco platforms and IOS versions supporting NetFlow

Enabling NetFlow Export

Enter global configuration mode on the router or MSFC, and issue the following commands for **each interface** on which you want to enable NetFlow:

```
interface {interface} {interface_number}
ip route-cache flow
bandwidth <kbps>
exit
```

In some recent IOS releases Cisco Express Forwarding has to be enabled. Issue the command `ip cef` in global configuration mode on the router or MSFC for this.

This enables NetFlow on the specified interface alone. Remember that on a Cisco IOS device, **NetFlow is enabled on a per-interface basis**. The `bandwidth` command is optional, and is used to set the speed of the interface in kilobits per second. Interface speed or link speed value is used to later calculate percentage utilization values in traffic graphs.

Exporting NetFlow Data

Issue the following commands to export NetFlow data to the server on which NetFlow Analyzer is running:

Command	Purpose
`ip flow-export destination {hostname|ip_address} 9996`	Exports the NetFlow cache entries to the specified IP address. Use the IP address of the NetFlow Analyzer server and the configured NetFlow listener port. The default port is 9996.
`ip flow-export source {interface} {interface_number}`	Sets the source IP address of the NetFlow exports sent by the device to the specified IP address. NetFlow Analyzer will make SNMP requests of the device on this address.
`ip flow-export version 5 [peer-as | origin-as]`	Sets the NetFlow export version to version 5. NetFlow Analyzer supports only version 5, version 7 and version 9. If your router uses BGP you can specify that either the origin or peer AS is included in exports - it is not possible to include both.
`ip flow-cache timeout active 1`	Breaks up long-lived flows into 1-minute fragments. You can choose any number of minutes between 1 and 60. If you leave it at the default of 30 minutes your traffic reports will have spikes. It is important to set this value to 1 minute in order to generate alerts and view troubleshooting data.
`ip flow-cache timeout inactive 15`	Ensures that flows that have finished are periodically exported. The default value is 15 seconds. You can choose any number of seconds between 10 and 600. However, if you choose a value greater than 250 seconds, NetFlow Analyzer may report traffic levels that are too low.
`snmp-server ifindex persist`	Enables ifIndex persistence (interface names) globally. This ensures that the ifIndex values are persisted during device reboots.

For more information on BGP reporting in NetFlow Analyzer, look up the section on Configuring NetFlow for BGP

Verifying Device Configuration

Issue the following commands in **normal (not configuration) mode** to verify whether NetFlow export has been configured correctly:

Command	Purpose
`show ip flow export`	Shows the current NetFlow configuration
`show ip cache flow`	These commands summarize the active flows and give an indication of how much NetFlow data the device is exporting
`show ip cache verbose flow`	

A Sample Device Configuration

The following is a set of commands issued on a router to enable NetFlow version 5 on the FastEthernet 0/1 interface and export to the machine 192.168.9.101 on port 9996.

```
router#enable
Password:*****
router#configure terminal
router-2621(config)#interface FastEthernet 0/1
router-2621(config-if)#ip route-cache flow
router-2621(config-if)#exit
router-2621(config)#ip flow-export destination 192.168.9.101 9996
router-2621(config)#ip flow-export source FastEthernet 0/1
router-2621(config)#ip flow-export version 5
router-2621(config)#ip flow-cache timeout active 1
router-2621(config)#ip flow-cache timeout inactive 15
router-2621(config)#snmp-server ifindex persist
router-2621(config)#^Z
router#write
router#show ip flow export
router#show ip cache flow
```

**repeat these commands to enable NetFlow for each interface*

Please note that NetFlow data export has to be enabled on all interfaces of a router in order to see accurate IN and OUT traffic. Suppose you have a router with interface A and B. Since NetFlow, by default, is done on an ingress basis, when you enable NetFlow data export on interface A, it will only export the IN traffic for interface A and OUT traffic for interface B. The OUT traffic for interface A will be contributed by the NetFlow data exported from interface B.

Even if you are interested in managing only interface A, please enable NetFlow data export on A and B. You may subsequently unmanage interface B from the License Management link.

Turning off NetFlow

Issue the following commands in global configuration mode to stop exporting NetFlow data:

Command	Purpose
`no ip flow-export destination {hostname|ip_address} {port_number}`	This will stop exporting NetFlow cache entries to the specified destination IP address on the specified port number
`interface {interface} {interface_number}`	This will disable NetFlow export on the specified interface. Repeat the commands for each interface on which you need to disable NetFlow.
`no ip route-cache flow`	
`exit`	

For further information on configuring your IOS device for NetFlow data export, refer Cisco's NetFlow commands documentation

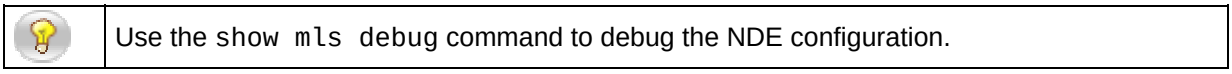
Configuring NDE on Catalyst 6000 Series Switches

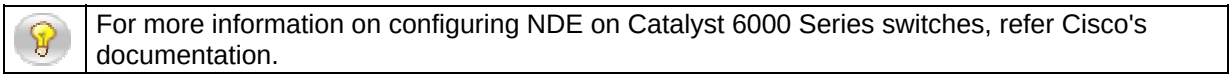
Follow the steps below to configure NDE on Catalyst 6000 Series switches

Enter privileged mode on the Supervisor Engine and issue the following commands to configure NDE:

Command	Purpose
`set mls nde {hostname|ip_address} 9996`	Specifies NetFlow Analyzer as the NDE collector and the configured Netflow listener port as the UDP port for data export of hardware-switched packets.
`ip flow-export destination {hostname|ip_address} 9996`	Specifies NetFlow Analyzer as the NDE collector and the configured Netflow listener port as the UDP port for data export of software-switched packets. *
`set mls agingtime long 64`	Breaks up long-lived flows into 1-minute fragments. This ensures that traffic graphs do not have spikes. It is important to set this value to 1 minute in order to generate alerts and view troubleshooting data.
`set mls agingtime 32`	Ensures that flows that have finished are periodically exported. Ensure that the set value is not too low, else NetFlow Analyzer may report traffic levels that are too low.
`set mls flow full`	This sets the flow mask to full flows. This is required to get useful information from the switch.
`set mls nde enable`	This enables NDE

**To monitor data and statistics about Layer 3 traffic that is switched in software by the MSFC, you must specify the NDE collector and UDP port on the MSFC. This requires that you enter the `ip flow-export destination` command on the MSFC.*





Configuring NDE on a Native IOS Device

To enable NDE on a Native IOS device, enter the configure mode on the Supervisor Engine, and follow the instructions for an IOS device. Then issue the following commands to enable NDE.

Configuring NDE

Enter privileged mode on the Supervisor Engine and issue the following commands to enable NDE:

Command	Purpose
`mls nde sender version 7`	Sets the export version. Version 7 is the most recent full export version supported by switches.
`set mls aging long 64`	Breaks up long-lived flows into 1-minute fragments. This ensures that traffic graphs do not have spikes. It is important to set this value to 1 minute in order to generate alerts and view troubleshooting data. .
`set mls aging normal 32`	Ensures that flows that have finished are periodically exported. A lower value may result in NetFlow Analyzer reporting traffic levels that are too low.

In order to put interface an routing information into the Netflow exports, issue the following commands depending on the Supervisor Engine.

Switch Configuration	Lowest IOS (MSFC) Level	Commands
Sup2 or 720	12.1.13(E)	`mls flow ip interface-full` `mls nde interface`
Sup1	12.1.13(E)	`set mls flow ip full`

This information is not available with IOS versions earlier than 12.1.13(E) on the Supervisor Engine 2 or 720

Configuring NDE on 4000 Series Switches

Follow the steps below to configure NDE on a 4000 Series switches.

The 4000 and 4500 series switches require a Supervisor IV with a NetFlow Services daughter card(WS-F4531) and IOS version 12.1(19)EW or above to support NDE.

Configure this device as for an IOS device, but **omit** the `ip route-cache flow` command on each interface. Then issue the following command:

```
ip route-cache flow infer-fields
```

This command ensures routing information is included in the flows. You will not enter the `ip route-cache flow` command on each interface.

A Sample Device Configuration

The following is a set of commands issued on a 4000 Series switch to enable NetFlow version 7 and export to the machine 192.168.9.101 on port 9996 using FastEthernet 0/1 as the source interface.

```
switch>(enable)ip flow-export destination 192.168.9.101 9996
switch>(enable)ip flow-export version 7
switch>(enable)ip flow-export source FastEthernet 0/1
switch>(enable)ip flow-cache timeout active 1
switch>(enable)ip route-cache flow infer-fields
```

Configuring NetFlow for BGP

The Border Gateway Protocol (BGP), defined in RFC 1771, provides loop-free interdomain routing between autonomous systems. (An autonomous system [AS] is a set of routers that operate under the same administration.) BGP is often run among the networks of Internet service providers (ISPs).

	In order to get AS info, you need to configure your router to include AS info. AS information collection is resource intensive, especially when configured for origin-AS. In case you are not interested in monitoring peering arrangements, disabling AS collection may improve NetFlow Analyzer performance.

Enabling BGP Routing

Enter the global configuration mode and issue the following commands to enable BGP routing and establish a BGP routing process:

Command	Purpose
`router bgp as-number`	Enables the BGP routing process, which places the router in router configuration mode
`network network-number [mask network-mask] [route-map route-map-name]`	Flags a network as local to this autonomous system and enters it to the BGP table

Configuring BGP Neighbors

BGP supports two kinds of neighbors: internal and external. Internal neighbors are in the same autonomous system; external neighbors are in different autonomous systems. Normally, external neighbors are adjacent to each other and share a subnet, while internal neighbors may be anywhere in the same autonomous system.

To configure BGP neighbors, issue the following command in router configuration mode:

Command	Purpose
`neighbor {ip-address|peer-group-name} remote-as as-number`	Specifies a BGP neighbor

BGP Neighbor Configuration Examples

The following example shows how BGP neighbors on an autonomous system are configured to share information.

```
router bgp 109
network 131.108.0.0
network 192.31.7.0
neighbor 131.108.200.1 remote-as 167
neighbor 131.108.234.2 remote-as 109
neighbor 150.136.64.19 remote-as 99
```

In the example, a BGP router is assigned to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 131.108.0.0 and 192.31.7.0 with the neighboring routers. The first router listed is in a different autonomous system; the second neighbor's `remote-as` router configuration command specifies an internal neighbor (with the same autonomous system number) at address *131.108.234.2* and the third neighbor's `remote-as` router configuration command specifies a neighbor on a different autonomous system.

Including AS Info in Netflow Exports

If you have configured BGP on your network, and want Netflow to report on autonomous systems (AS info), issue the following command on the router in global configuration mode:

Command	Purpose
`ip flow-export destination {hostname|ip_address} 9996`	Exports the Netflow cache entries to the specified IP address. Use the IP address of the NetFlow Analyzer server and the configured Netflow listener port. The default port is 9996.
`ip flow-export {version}[peer-as | origin-as]`	Exports NetFlow cache entries in the specified version format (5 or 7). If your router uses BGP, you can specify that either the origin or peer ASs are included in exports – it is not possible to include both.

Juniper Devices (cflowd/J-Flow)

Configuring flow exports on Juniper Routers

This section gives the steps to configure cflowd/J-Flow export on Juniper devices.To enable sampling and to export the flow records to specific destination address, follow the below command:

```
forwarding-options {
  sampling {
     input {
        family inet {
           rate 100;
           run-length 9;
           max-packets-per-second 7000;
        }
     }
     output {
        cflowd <destination address>{
           port <port number>;
           source-address <source address>;
           version <version number>;
           no-local-dump;
           autonomous-system-type origin;
        }
     }
  }
}
```

To enable packet sampling on the particular interface(s), from which flow analyzis to be done follow the below steps:

```
interfaces {
   ge-1/3/0 {
      vlan-tagging;
      unit 101 {
         vlan-id 101;
         family inet {
            sampling {
               input;
               output;
            }
            address 206.80.253.26/25
         }
      }
   }
}
```

For more information, refer here and this link (*to configure V9 Template record*).

Huwaei/3com devices(Netstream)

Configuring NetStream Export

On H3C routers:

Please refer to this link to configure Netstream exports on H3C devices.

On Huwaei Devices:
Follow the below command to enable NetStream on Huwaei devices

ip netstream export host {hostname|ip_address} 9996

This exports the NetStream exports to the specified IP address. Use the IP address of the NetFlow Analyzer server and the configured listener port. The default port is 9996.

ip netstream export source interface {interface name}

Sets the source IP address of the NetStream exports sent by the device to the specified IP address. NetFlow Analyzer will make SNMP requests of the device on this address. For enabling Netstream on the desired interface, please execute the following command

ip netstream inbound

Nortel Devices(IPFIX)

Configuring IPFIX Export

According to Nortel Devices, Internet Protocol Flow Information eXport (IPFIX) has evolved as an improvement upon the Netflow V9 protocol. *It is an upcoming standard that has been proposed by an IETF Working Group - http://www.ietf.org/html.charters/ipfix-charter.html. IPFIX is an effort to standardize on architecture for IP flow measurement and export. In an IPFIX model, an exporter such as a switch or router collects IP flows and then exports the IP flow information using a transport protocol to a collection server or servers. An IP flow is defined as a set of packets over a period of time that has some common properties.*

Please refer to the PDF document published by Nortel Devices in this page to configure IPFIX flow exports from your Nortel Devices.

sFlow Reporting

What is sFlow ?

According to sFlow.org, *sFlow® is an industry standard technology for monitoring high speed switched networks. It gives complete visibility into the use of networks enabling performance optimization, accounting/billing for usage, and defense against security threats.*

It further says, *sFlow is a sampling technology that meets the key requirements for a network traffic monitoring solution:*

- **sFlow is an industry standard** with interoperable implementations provided by a wide range of network equipment and software application vendors
- ***sFlow provides a network-wide view*** *of usage and active routes. It is a scalable technique for measuring network traffic, collecting, storing, and analyzing traffic data. This enables tens of thousands of interfaces to be monitored from a single location*
- ***sFlow is scalable****, enabling it to monitor links of speeds up to 10Gb/s and beyond without impacting the performance of core internet routers and switches, and without adding significant network load*
- ***sFlow is a low cost solution****. It has been implemented on a wide range of devices, from simple L2 workgroup switches to high-end core routers, without requiring additional memory and CPU*

sFlow Supported Devices

Which devices support sFlow ?

The following devices are capable of exporting sFlow :

AlaxalA Networks

- AX7800R
- AX7800S
- AX7700R
- AX5400S

Alcatel

- OmniSwitch 6850
- OmniSwitch 9000

Allied Telesis

- SwitchBlade 7800R series
- SwitchBlade 7800S series
- SwitchBlade 5400S series

Comtec Systems

- !-Rex 16Gi & 24Gi & 24Gi-Combo

Extreme Networks

- Alpine 3800 series
- BlackDiamond 6800 series
- BlackDiamond 8800 series
- BlackDiamond 10808
- BlackDiamond 12804C
- BlackDiamond 12804R
- Summit X450 Series
- Summit i series

Force10 Networks

- E series

Foundry Networks

- BigIron series
- FastIron series
- IronPoint series
- NetIron series
- SecureIron series
- ServerIron series

Hewlett-Packard

- ProCurve 2800 series
- ProCurve 3400cl series

- ProCurve 3500yl series
- ProCurve 4200vl series
- ProCurve 5300xl series
- ProCurve 5400zl series
- ProCurve 6200yl series
- ProCurve 6400cl series
- ProCurve 9300m series
- ProCurve Routing Switch 9408sl

Hitachi

- GR4000
- GS4000
- GS3000

NEC

- IP8800/R400 series
- IP8800/S400 series
- IP8800/S300 series

Enabling sFlow

How do I enable sFlow ?

If your device supports sFlow, then you will have to enable sFlow on each of the interfaces that you want to collect flow statistics on.

Enabling sFlow on various devices

Foundry Networks switch

```
foundry2402#enable
Password:*****
foundry2402#configure terminal
foundry2402(config)# interface ethernet 10
foundry2402(config-if-e100-10)#sflow forwarding
foundry2402(config-if)#exit foundry2402(config)# sflow enable
foundry2402(config)# sflow destination 192.168.0.2 9996
foundry2402(config)# sflow sample 256
foundry2402(config)# sflow polling-interval 10
```

Please note that the part in red has to be repeated for each interface individually.

For more information on Foundry devices configuration refer to www.foundrynet.com

Force10 switch

```
force#enable
Password:*****
force#configure terminal
force(config-interface)#sflow enable
[ This command has to be repeated for all interfaces. ]
force(config)#sflow destination 192.168.0.2 9996 agent-addr 192.168.1.2
force(config)# sflow sample 256
force(config)# sflow polling 10
```

For more information on Force10 devices refer to www.force10networks.com

Extreme Networks switch

Please refer to the following documentation for configuring sFlow on Extreme Networks switch

- http://www.extremenetworks.com/libraries/whitepapers/WPsFlow_1247.pdf
- For enabling sFlow on the port use the following command. This has to be repeated for all the ports.

```
extreme#enable sflow port
```

For more information on Extreme Network devices refer to www.extremenetworks.com

Hewlett-Packard ProCurve switches

```
hp#enable
Password:*****
hp#configure terminal
hp# sflow 1 sampling A1,A2,A2 256 [ sflow 1 sampling <modules> <sampling rate>]
hp# sflow 1 destination 192.168.0.2 9996
```

The above commands work only on latest HP devices.

sFlow can be enabled on some of the HP switches only through SNMP. We provide two script files for enabling and disabling sFlow on HP switch.

The script files **SFlowEnable.bat** / **SFlowEnable.sh** and **SFlowDisable.bat** / **SFlowDisable.sh** are present under <NetFlow_Analyzer_HOME>/troubleshooting folder.

For **enabling sFlow** you need to provide the below command:

```
SFlowEnable.bat switchIp snmpPort snmpWriteCommunity collecorIP collectorPort samplingRat
```

An example,

```
SFlowEnable.bat Hp2824 161 private 192.168.3.1 9996 25
```

For **disabling sFlow** you need to provide the below command:

```
SFlowDisable.bat switchIp snmpPort snmpWriteCommunit
```

An example,

```
SFlowDisable HpProcurve 161 private
```

For more information on HP devices refer to www.hp.com

Different Views in NFA

Different Views in NetFlow Analyzer

Once NetFlow Analyzer has been successfully set up and started in your network, the next thing to do is to start receiving Netflow exports from routing devices on your network.

	The Configuring Cisco Devices section contains useful information on how to configure Netflow export on different Cisco routers and switches. The sFlow section contains useful information on configuring sFlow.

As soon as you log in to the NetFlow Analyzer web client, you will see the **Global View - Dashboard View**. This view shows you information on interfaces sending Netflow and sFlow exports, AS info, as well as traffic information for all IP groups created so far. The Dashboard is populated as soon as Netflow or sFlow data is received from any interface.

The Global View is divided into three tabs

1. The **Network Snapshot View** which lists the top devices, top interfaces and top IP Groups
2. The **Interface View** which lists all the interfaces from which Netflow or sFlow exports are received
3. The **Autonomous System View** which lists all the autonomous systems configured with each router

From any tab, click the  icon to return to the Global View.

Network Snapshot View

The **Network Snapshot View** is the default view when the user logs in to NetFlow Analyzer application. The time period for which the report is shown can be modified using the **Select Period** . The time period choosen could be one of - Last Hour, Last 6 Hours, Today and Last 24 Hours.

It displays details categorized under the following heads.

1. Top Devices by Speed
2. Top Interfaces by Speed
3. Top Interfaces by Utilization
4. Top IP Groups by Speed
5. Top IP Groups by Utilization

The top 5 Interfaces/ IP groups are listed in each category, as the case may be.

Top Devices by Speed

The Top Devices by Speed categorization lists the top 5 devices (routers/switches) on the basis of speed. is shown against each device name. Details of the Maximum Speed, Average Speed, Average Voulme, percentage utilization is shown against each device name. The Pie chart gives the representation of the share of the top devices as a percentage. Clicking on the region of a pie-chart gives details at the interface level for the device chosen. The same can be seen by clicking on the Device Name listed under the heading **Device Name**. The rectangular plot alongside the piechart gives the 1 Minute Average plot of speed Vs time.

Top Interfaces by Speed

The Top Interfaces by Speed categorization lists the top 5 interfaces (globally) on the basis of speed. Details such as the Device Name(on which the interface resides), the In and Out speeds on the Interface are listed. By clicking on any Interface Name, it is possible to further drill down to see more details on speed related information on this interface.

Top Interfaces by Utilization

The Top Interfaces by Utilization categorization lists the top 5 interfaces (globally) on the basis of Utilization. Details such as the Device Name(on which the interface resides), the In and Out Utilization on the Interface are listed. By clicking on any Interface Name, it is possible to further drill down to see more details on the utilization information on this interface.

Top IP Groups by Speed

The Top IP Groups by Speed categorization lists the top 5 IP Groups (globally) on the basis of speed. Details on the In and Out speeds on the IP Group are listed. By clicking on any IP Group Name, it is possible to further drill down to see more speed related details on the IP Group.

Top IP Groups by Utilization

The Top IP Groups by Utilization categorization lists the top 5 IP Groups (globally) on the basis of Utilization. Details on the In and Out utilization values on the IP Groups are listed. By clicking on any IP Group Name, it is possible to further drill down to see more utilization related details on the IP Group.

The purpose of icons and buttons in the Network Snapshot View is explained below.

Icon/ Button	Purpose
 (near Refresh this page)	Click this icon, to set the time period for refreshing the page contents.

Dashboard Interface View

The **Interface View** tab displays information on all interfaces from which NetFlow exports are received.

The default **Router List** shows all the routers and interfaces from which NetFlow exports have been received so far, along with specific details about each interface.
The default view shows the first router's interfaces alone. The interface names can be sorted based on usage. The remaining **routers'** interfaces are hidden. Click the **[Show All]** link to display all **routers'** interfaces on the Dashboard. Click the **[Hide All]** link to hide all interfaces and show only the router names in the Router List.

You can set filters on the Dashboard view to display only those interfaces whose incoming or outgoing traffic values exceed a specified percentage value. Click the **[Filter]** link to specify minimum percentage values for IN or OUT traffic. Click the **Set** button for the changes to take effect. The filter settings are then displayed beside the **[Filter]** link. Click the icon at any time to clear the filter settings and display all interfaces on the Dashboard again.

Click on the Set SNMP link next to "Router Name" to set SNMP parameters at a global level or at an individual router level.

By clicking on the **Select Period**, the time period choosen could be one of - Last Hour, Last 6 Hours, Today and Last 24 Hours. Reports corresponding to the chosen time period is shown in the Dashboard View.

The purpose of icons and buttons in the Router List is explained below.

Icon/ Button	Purpose
	Click this icon, or on the router name, to view the interfaces corresponding to the router
	Click this icon to hide the interfaces corresponding to the router
 (before Router Name)	Click this icon to change the display name of the device
 (before Interface Name)	Click this icon before the interface name to change the display name of the interface, or its link speed(IN and OUT (in bps)).
 (near Refresh)	Click this icon, to set the time period for refreshing the page contents.
	Click this link to troubleshoot an interface. You can troubleshoot only one interface at a time. Note: Troubleshooting results are shown directly from raw data. Hence results depend on the raw data retention time period set in Settings
	Indicates that NBAR report is available for the interface
	Click on this icon to have a preview of the traffic graphs without drilling down in to each interface
	Indicates that CBQoS report is available for the interface

The Interface Name column lists all the interfaces on a discovered device. Click on an interface to view the traffic details for that interface.

The Status column indicates the current status of that interface.

Icon	Description
	The Status of the interface is unknown and no flows have been received for the past 10 minutes. The interface is not responding to SNMP requests.
	The interface is responding to SNMP requests and the link is up, but no flows have been received for the past ten minutes.
	The link is up, and flows are being received.
	The interface is responding to SNMP requests and the link is down and no flows are being received.

The IN Traffic and OUT Traffic columns show the **utilization** of IN and OUT Traffic on the respective interfaces for the past one hour. You can click on the IN Traffic or OUT traffic bar to view the respective application traffic graph for that interface. Use the Custom Report link to generate custom reports. Set the value in Refresh this Page to inform the application how frequently the refresh has to be done to fetch the most recent data.

More Reports

Click on More Reports to Compare Device(s) over various time period(s) and to Generate Report based on custom defined criterion.

Compare Devices

Compare Devices feature lets the user Compare multiple devices for the same time period or Compare the same Device over different time periods. eg: Every Day Report, Every Hour Report, Every Week Report, Every Month Report.

Field	Purpose/Description
Report Type	The report type could be one of : • Compare Multiple Devices over the same time period (or) • Compare same device over different time periods as the case may be.
Select Period	When the Report Type is chosen as - Compare Multiple Devices over the same time period, the available Periods are Last Hour, Last 6 Hour, Today, Last 24 Hours, Yesterday, Last Week, Last Month, Last Quarter or Custom Selection. Custom Selection lets one choose the time period for which one desires the report to be generated. When the Report Type is chosen as -Compare same device over different time periods, the available Periods are Every Day Report, Every Hour Report, Every Week Report, Every Month Report.
Select Device(s)	This allows the user to select the device(if the same device is to be compared over various time periods) or the set of devices (that are to be compared for a single time period). The Select Devices option allows the user to select the devices in terms of Interface or IP Group (By default the top 10 interfaces or IP Group by utilization are chosen) which can be modified by clicking on the Modify button
Generate Report	The Generate Report invokes the report for the defined criteria. Report Options: The Report Options could be chosen to be one of

Field	Purpose/Description
	• Show Speed • Show Utilization • Show Packets
Maximize	When the Generate Report option is invoked, the filter condition frame is minimized to offer a better view of the graph (report) without scrolling. The filter frame can be restored by using the Maximize button.
Minimize	The Minimize button can be used to minimize the Filter Frame for a better view of the report (graph) generated without scrolling

Search Devices
The **Search** link lets you set criteria and view specific details about the traffic across the network on various interfaces. Data to generate this report is taken directly from aggregated data.

Upon clicking the Search link a pop-up with provision to Select Devices & set criteria comes up. In the pop-up window that opens up, click the **Select Devices** link to choose the interfaces on which the report should be generated.

Under Search Criteria, enter the criteria on which traffic needs to be filtered. You can enter any of the following criteria to filter traffic:

- Source/Destination Address
- Source/Destination Network
- Source/Destination Nodes
- Application
- Port/Port Range

The **From** and **To** boxes let you choose custom time periods for the report. Use the  icon to select the date and time easily. Use the **IN/OUT** box to display values based on IN traffic, OUT traffic, or both IN and OUT traffic. The **View per page** lets you choose how many results to display.

Once you select all the desired criteria, click the **Generate Report** button to display the corresponding traffic report. The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values. You can also sort the data displayed either by Number of packets or Bytes.

Dashboard AS View

The **Autonomous System View** tab displays information on all the autonomous systems (AS) to which a router belongs, along with traffic details for each AS.

	In order to get AS info in this view, you need to configure your router to include AS info. AS information collection is resource intensive, especially when configured for origin-AS. In case you are not interested in monitoring peering arrangements, disabling AS collection may improve NetFlow Analyzer performance.

The **Router List** displays each router along with the AS to which it belongs. Click on the AS Name to view the traffic report for that AS. The Dashboard also shows the organization to which the AS belongs, and the amount of incoming and outgoing traffic for the past one hour.

The purpose of icons and buttons in the Router List are explained below

Icon/ Button	Purpose
	Click this icon, or on the router name, to view the autonomous systems to which this router belongs
	Click this icon to hide the AS corresponding to a router
	Click this icon before the router name to change the display name of the device, its SNMP community string, or its SNMP port
 (near Refresh this page)	Click this icon, to set the time period for refreshing the page contents.
	Click this icon to see the - Last 1 Hour report, on incoming and outgoing traffic for that AS for the past one hour
	Click this icon to start AS collection
	Click this icon to stop AS collection

Google Map View

Google maps feature lets you physically locate your network resources on a map. This enables network administrators to have a feel of how distributed their network is and more importantly in a quick and easy drill down to resource-specific information. Information on up to 3 top interfaces linked to a router is shown in the map. NetFlow Analyzer, by using google maps, lets you position your devices on a map for a graphical presentation. You need to obtain a Google API Key in order to set up this. The steps to obtain one is elaborated below.

Generating the Google Maps API key

The Google Maps API key is necessary to access the Google Map feature. You can get it by following the below steps:

- Click on the Google Map View tab - An alert message pops up which tells you the URL at which you can generate a key for your access
- Proceed to the **Configuring Google Map View** screen
- Follow **Step 1** - Click on the "**Click Here**" link
- A new window opens up which reads "Sign up for the Google Maps API".
    - Agree to the terms and conditions set forth in that page
- Specify the URL at which you will be accessing the application
- Click on the "Generate API Key" button
- A window will appear with the message " Your Key is" and the key below it
- Copy the key and paste it in the place provided in the application (in **Step 2**)
- Click on "**Update**"

Once the key is pasted a map can be seen with the devices located on it. Refer to Settings to make any changes to the display.

Please note that, NetFlow Analyzer allows you to store only one key for a particular installation. In case you obtain the key using http://<12.12.12.12>:8080 and try to access it using http://<servername>:8080, you will not be able to access the Google Map View and you may be prompted to obtain a fresh key. We recommend that you use the IP address / DNS name when you obtain the key and access NetFlow Analyzer using the same URL.

IP Groups View

Information on IP groups created so far, is displayed below both the Global View tabs. This is also displayed when the **All Groups** link is clicked on the **IP Groups** pane on the left.
Initially when no IP groups have been created, you will simply see a status message "**No IP groups have been configured**".

The **IP Group List** shows all the IP groups that have been created so far. Click the **View Description** link to view descriptive information on all IP groups created. Alternatively you can click the **View Description** link against each IP group to view descriptive information on that IP group alone.

Click the IP Group name to view traffic graphs specific to that IP group. From the traffic graph, you can navigate to see the top applications, top hosts, and top conversations in this IP group.

The **IN Traffic** and **OUT Traffic** columns show the volume of incoming and outgoing traffic in the IP group generated over the past one hour. You can click on the IN Traffic or OUT traffic bar to view the respective application traffic report.

Click the  icon to see a consolidated traffic report for the respective IP group. This report shows you all the details about incoming and outgoing traffic in this IP group in a single report.

Click the  icon to see the speed graph for the particular IP group.

View NetFlow Traffic Statistics of an Interface from OpManager

With NetFlow Analyzer plug-in from OpManager you can view the NetFlow traffic statistics of an interface for the current day. To view the NetFlow traffic statistics from OpManager, go to the snapshot page of the interface on which NetFlow is enabled. The interfaces that are NetFlow enabled are displayed with the icon. Click on the icon to view the NetFlow traffic statistics. The IN and OUT traffic contributed by the interfaces are displayed:

- Application
- Source
- Destination
- QoS
- Conversation
- NBAR

Viewing Traffic Reports

NetFlow Analyzer generates traffic reports in real-time, as soon as NetFlow data is received from an interface.

The traffic reports in NetFlow Analyzer include information on:

- Traffic Trends
- Top Applications
- Top Hosts
- Top Conversations

Apart from these pre-defined reports, Search Report let you define criteria and generate specific reports on network activity. Consolidated Reports show you overall traffic statistics for an interface or AS as applicable. Troubleshooting Reports let you troubleshoot an interface using raw data directly.

Click the  icon or the **Troubleshoot** link in the page to troubleshoot this interface.

Real-time Traffic Graphs

NetFlow Analyzer generates traffic graphs as soon as Netflow data is received. The **Traffic** tab shows real-time traffic graphs for incoming and outgoing traffic. Depending on which link was clicked, you can see traffic graphs for an interface or IP group.

Tabs above the traffic graph, let you view the graph in terms of volume of traffic, speed, link utilization, and number of packets received.

	The Packets tab shows the number of actual packets of traffic data received. This information is included in exported Netflow data.

You can see traffic graphs for different time periods by choosing the appropriate values from the Time Period box. Use the **From** and **To** boxes to choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show Report** button to display the appropriate traffic report.

The table below the graph shows the legend, along with total, maximum, minimum, and average traffic values for this interface or IP group, for the selected time period.

The **Traffic IN Details** and the **Traffic OUT Details** show sampled values of traffic generated over the selected time period.

Time Filters

The default graph is for the "Last Day". You can choose to see hour-based data in the traffic graphs for daily and weekly reports. To do this, first select the **Last Day Report** or **Last Week Report** option in the top time selection bar. When the respective traffic graph is displayed, the table below the graph includes the  icon next to the **Category** label.

Click the  icon to specify the hourly time interval for which you want to see traffic graphs. Click the **Show** button to set the filter and see hour-based values in the traffic graph as well as the table below. Click the **Reset** button to turn the filter off and switch to the regular traffic graphs.

95-th Percentile

The 95th percentile is the number that is greater than 95% of the numbers in a given set. The reason this statistic is so useful in measuring data throughput is that it gives a very accurate picture of the maximum traffic generated on an interface. This is a standard measure that is used for interpreting the performance data.

The 95th Percentile is the highest value left when the top 5% of a numerically sorted set of collected data is discarded. It is used as a measure of the peak value used when one discounts a fair amount for transitory spikes. This makes it markedly different from the average. The following example would help you understand it better.

Consider if the data collected for CPU Utilization is 60,45,43,21,56,89,76,32,22,10,12,14,23,35,45,43,23,23,43,23 (20 points). This list is sorted in descending order and a single top value, 89, is discarded. Since 1 consitutes 5% of 20, we discarded 1 value in this case. The highest value in the remaining list, 76, is the 95th percentile.

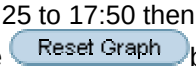
Selectable Graph

NetFlow Analyzer brings you the added advantage of drill-down to the traffic graphs presented. As you hover the mouse over the plot-area you can see a "+ " - cross-hair icon. Click on an area of the graph and holding the mouse down, drag it to the point(time period), you wish to further drill down to.

For example : Having chosen a Last week report you could choose to study two specific days by selecting them. You could further drill down on until the time period you have chosen is more than 1 minute. The 

button take you to a time period depending on the time difference between the From time and the system time.

Illustration

If you choose Last Hour Report at 18:15 hours, then a graph with a plot of data from 17:15 to 18:15 is shown. If you choose the time period 17: 25 to 17:50 then a corresponding graph with 1 Minute Average is shown. When you click on the 

button the screen changes to the Last Hour report. (as the time difference between the From Time 17:25 and system time 18:20 is less than 1 hour)

Thus depending on the time difference you are either taken to the Last Hour or Last Day or Last Week or Last Month or Last Quarter graph.

Top Applications

The **Applications** tab shows you the top applications and top protocols for the selected time period. The default view shows the **Top ApplicationIN Report**. This report shows the distribution of incoming traffic application-wise.

Choose between **IN** and **OUT** to display the application-wise distribution of incoming or outgoing traffic respectively.

The Time Period box lets you choose between last hour, last day, last week, last month, and last quarter's traffic graphs. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show** button to display the appropriate application traffic report.

The table below the graph shows the distribution of traffic per application. You can see what application caused how much traffic, and how much of the total bandwidth was occupied by that application.

The Show Ports Link next to an application name indicates that that application is not identified by NetFlow Analyzer. When you click on Show Ports Link, a window opens up showing the port and protocol details for this application. If it is a valid application you can then add it to the list of applications in the Application Mapping page.

	The Show Ports Link will be displayed next to an unknown application only in the Last Hour report.

Click on an application's name to see the Top Conversations that contributed to this application's traffic.

The **Show** box above this table lets you choose how many applications need to be displayed. You can set the maximum value for this option from the Settings page.

The pie chart below this table shows what percentage of bandwidth is being used by each application. The  icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can click the  icon to save the pie chart as a PDF file.

Viewing Top Protocols

Click the  icon or the **Protocol Distribution** link to see the top protocols for the selected interface or IP group, in a new window.

Choose between **IN** and **OUT** to display the protocol-wise distribution of incoming or outgoing traffic respectively.

	This report sorts traffic based on the protocol used, while the Application IN/OUT Report sorts traffic based on the application, i.e., the combination of port and protocol.

Click on a protocol's name to see the Top Conversations that used this protocol. The **Show** box above this table lets you choose how many applications need to be displayed. You can set the maximum value for this option from the Settings page.

The pie chart below this table shows what percentage of bandwidth is being used by each protocol. The  icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can click the  icon to save the pie chart as a PDF file.

Top Hosts

The **Source** tab shows the top source hosts contributing to traffic in the selected time period. The default view shows the **Top SourceIN Report**.

The **Destination** tab shows the top destination hosts contributing to traffic in the selected time period. The default view shows the **Top DestinationIN Report**.

Choose between **IN** and **OUT** to display the top hosts in incoming or outgoing traffic.

	When you drill down from an IP group, traffic is unidirectional, and hence the IN and OUT options are not available

The Time Period box lets you choose between last hour, last day, last week, last month, and last quarter's traffic graphs. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show** button to display the appropriate source or destination traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values.

Click the **Show Network** link to see the network-wise top sources and destinations.
Ex: 192.168.4.0 / 24 . Here 192.168.4.0 is the IP address and 24 is the network mask.

The **Show** box above this table lets you choose how many hosts need to be displayed. You can set this value from the Settings page.

The pie chart below this report shows what percentage of bandwidth is being used by each host. The  icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can click the  icon to save the pie chart as a PDF file.

QoS

QoS or Quality of service is the most important factor that determines how effectively the available enterprise bandwidth is being used in the WAN. It is also an index of the overall User Experience of the available Bandwidth.

The QoS feature by default lists out the Top DSCP IN Report.Clicking on the Show Applications link lists out the various DSCP values along with the list of applications that comprise the DSCP. It also list out details on Traffic and percentage utilization of the total traffic by each of the applications and the DSCP group as a whole. Clicking on the icon next to the DSCP value gives a detailed traffic graph in a pop-up screen.

DSCP

The DSCP Groups can be viewed by clicking on the View DSCP Group link. If no DSCP Groups have been created earlier, then an appropriate message is displayed and the user is prompted to create a DSCP group. The bottom of the page lists the Top DSCP IN Traffic as a Pie Distribution.

The time period for which the report is shown can be controlled by using the time selection bar at the top.

TOS

Because the Internet by itself has no direct knowledge of optimizing the path for a particular application or user, the IP protocol provides a facility for upper layer protocols to convey hints to the Internet Layer about how the tradeoffs should be made for a particular packet. This facility is the "Type of Service" facility, abbreviated as the "TOS facility".

The TOS facility is one of the features of the Type of Service octet in the IP datagram header. The Type of Service octet consists of three fields. The first 3 bits (0,1,2) are for the first field, labeled "Precedence" , intended to denote the importance or priority of the datagram. The second field, labeled "TOS" , denotes how the network should make tradeoffs between throughput, delay, reliability, and cost.The last field, labeled "MBZ" (for "must be zero") above, is currently unused. The originator of a datagram sets this field to zero (unless participating in an Internet protocol experiment which makes use of that bit). Routers and recipients of datagrams ignore the value of this field.This field is copied on fragmentation.

Specification of the TOS Field

The semantics of the TOS field values (expressed as binary numbers):

1000	**minimize delay**
0100	**maximize throughput**
0010	**maximize reliability**
0001	**minimize monetary cost**
0000	**normal service**

The values used in the TOS field are referred to as "TOS values", and the value of the TOS field of an IP packet is referred to as the "requested TOS". The TOS field value 0000 is referred to "default TOS." Because this specification redefines TOS values to be integers rather than sets of bits, computing the logical OR of two TOS values is no longer meaningful. For example, it would be a serious error for a router to choose a low delay path for a packet whose requested TOS was 1110 simply because the router noted that the former "delay bit" was set.

Although the semantics of values other than the five listed above are not defined , they are perfectly legal TOS values, and hosts and routers must not preclude their use in any way. Only the default TOS is in any way special. A host or router need not make any distinction between TOS values

For example, setting the TOS field to 1000 (minimize delay) does not guarantee that the path taken by the datagram will have a delay that the user considers "low". The network will attempt to choose the lowest delay path available, based on its (often imperfect) information about path delay. The network will not discard the datagram simply because it believes that the delay of the available paths is "too high" (actually, the network manager can override this behavior through creative use of routing metrics, but this is strongly discouraged: setting the TOS field is intended to give better service when it is available, rather than to deny service when it is not).

Use of the TOS Field in Routing

Both hosts and routers should consider the value of the TOS field of a datagram when choosing an appropriate path to get the datagram to its destination.The mechanisms for doing so are discussed in this section.

Whether a packet's TOS value actually affects the path it takes inside a particular routing domain, is a choice made by the routing domain's network manager. In many routing domains the paths are sufficiently homogeneous in nature that there is no reason for routers to choose different paths based up the TOS field in a datagram. Inside such a routing domain, the network manager may choose to limit the size of the routing database and of routing protocol updates by only defining routes for the default (0000) TOS.

Neither hosts nor routers should need to have any explicit knowledge of whether TOS affects routing in the local routing domain.

Inherent Limitations:

The most important of all the inherent limitations is that the TOS facility is strictly an advisory mechanism. It is not an appropriate mechanism for requesting service guarantees.There are two reasons why this is so:

- Not all networks will consider the value of the TOS field when deciding how to handle and route packets.Partly this is a transition issue: there will be a (probably lengthy) period when some networks will use equipment that predates this specification. Even long term, many networks will not be able to provide better service by considering the value of the TOS field. For example, the best path through a network composed of a homogeneous collection of interconnected LANs is probably the same for any possible TOS value. Inside such a network, it would make little sense to require routers and routing protocols to do the extra work needed to consider the value of the TOS field when forwarding packets.
- The TOS mechanism is not powerful enough to allow an application to quantify the level of service it desires. For example, an application may use the TOS field to request that the network choose a path which maximizes throughput, but cannot use that mechanism to say that it needs or wants a particular number of kilobytes or megabytes per second. Because the network cannot know what the application requires, it would be inappropriate for the network to decide
  to discard a packet which requested maximal throughput because no "high throughput" path was available.

Top Conversations

The **Conversation** tab shows the top conversations contributing to traffic in the selected time period.

Choose between **IN** and **OUT** to display the top conversations in incoming or outgoing traffic.

The Time Period box lets you choose between last hour, last day, last week, last month, and last quarter's traffic graphs. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show** button to display the appropriate conversation traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS names.

Click the **Show Network** link to see the network-wise top conversations
Ex: 192.168.4.0 / 24 . Here 192.168.4.0 is the IP address and 24 is the network mask. .

The **Show** box above this table lets you choose how many conversations need to be displayed. You can set this value from the Settings page.

The **Group by** box lets you group conversations by source, destination, or application. The default list shows the conversations sorted in descending order of number of bytes of traffic.
The pie charts below this report show the top sources, destinations, and conversations contributing to traffic for the selected time period. The  icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can click the  icon to save the pie chart as a PDF file.

AS Traffic Reports

The Traffic report for autonomous systems shows the amount of incoming and outgoing traffic for that AS, over the past one hour.

Tabs above the traffic graph let you view the graph in terms of volume of traffic, speed, and number of packets received.

You can see traffic graphs for different time periods by choosing the appropriate values from the Time Period box. Use the **From** and **To** boxes to choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show Report** button to display the appropriate traffic report.

The table below the graph shows the legend, along with total, maximum, minimum, and average traffic values for this AS for the selected time period.

The **Traffic IN Details** and the **Traffic OUT Details** show sampled values of traffic generated over the selected time period.

Troubleshooting

The **Troubleshoot** link lets you set criteria and view specific details about the traffic across a single interface. Data for Troubleshooting reports is taken directly from raw data. Which means that Troubleshooting reports will be available only for the maximum time period for retaining raw data, configured under Settings.

Click the icon against an interface on the Dashboard Interface View, or the **Troubleshoot** link present above the traffic graphs for an interface, to open a popup with options to set criteria for viewing reports. In the pop-up window that opens up, click the **Select Devices** link to change the interface that you want to troubleshoot.

Under Search Criteria, enter the criteria on which traffic needs to be filtered. You can enter any of the following criteria to filter traffic:

- Source/Destination Address
- Source/Destination Network
- Source/Destination Nodes
- Application
- Port/Port Range

The **From** and **To** boxes let you choose custom time periods for the report. Use the icon to select the date and time easily. Ensure that the time period selected, falls within the Raw Data Retention Period set under Settings, otherwise graphs will show no data.

Use the **IN/OUT** box to display values based on IN traffic, OUT traffic, or both IN and OUT traffic. The **Show** box lets you choose how many results to display. You can set this value from the Settings page.

Once you select all the desired criteria, click the **Generate Report** button to display the corresponding traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values. You can also choose to print this report by clicking the icon or the **Print** link.

Consolidated Reports

Consolidated reports let you see all the traffic details for an interface or IP group at one glance. You can then print this report or save it as a PDF file.

Click the **Consolidated Report** link to see all traffic details for an interface at one glance. The same report can be accessed from the Global Dashboard when the icon against an interface or IP group is clicked.

The Custom Selection box lets you select different time periods for the traffic data.

> The **1 Hour Report** and **1 Day Report** options show you traffic details over the past one hour and one day respectively.
> The **8AM to 8PM** option shows you traffic details from 8 a.m. to 8 p.m. of the previous day. This is a peak hour report, based on the normal working hours of an enterprise.

Apart from these options, the **From** and **To** boxes let you choose custom time periods for the report. Use the icon to select the date and time easily. Once you select the desired time period, click the **Show Report** button to display the corresponding consolidated report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS names. You can also choose to save the report as a PDF file by clicking the icon, or print it by clicking the Print icon.

Compare Report - NetFlow Analyzer Global Report

Compare Devices feature lets the user Compare multiple devices for the same time period or Compare the same Device over different time periods. eg: Every Day Report, Every Hour Report, Every Week Report, Every Month Report.

Field	Purpose/Description
Report Type	The report type could be one of : • Compare Multiple Devices over the same time period (or) • Compare same device over different time periods as the case may be.
Select Period	When the Report Type is chosen as - Compare Multiple Devices over the same time period, the available Periods are Last Hour, Last 6 Hour, Today, Last 24 Hours, Yesterday, Last Week, Last Month, Last Quarter or Custom Selection. Custom Selection lets one choose the time period for which one desires the report to be generated. When the Report Type is chosen as -Compare same device over different time periods, the available Periods are Every Day Report, Every Hour Report, Every Week Report, Every Month Report.
Select Device(s)	This allows the user to select the device(if the same device is to be compared over various time periods) or the set of devices (that are to be compared for a single time period). The Select Devices option allows the user to select the devices in terms of Interface or IP Group (By default the top 10 interfaces or IP Group by utilization are chosen) which can be modified by clicking on the Modify button
Generate Report	The Generate Report invokes the report for the defined criteria. Report Options: The Report Options could be chosen to be one of • Show Speed • Show Utilization • Show Packets
Maximize	When the Generate Report option is invoked, the filter condition frame is minimized to offer a better view of the graph (report) without scrolling. The filter frame can be restored by using the Maximize button.
Minimize	The Minimize button can be used to minimize the Filter Frame for a better view of the report (graph) generated without scrolling

Search Report

Custom Reports let you set several criteria and view specific reports. This is especially useful in finding out the bandwidth utilization of a specific host or application. Custom reports can also tell you details about a certain application and which hosts are using it, thereby helping to troubleshoot, and even detect virus activities.

Click the  icon or the **Custom Report** link on the Dashboard to to set criteria and view custom reports. In the pop-up window that opens up, click the **Select Devices** link to select the routers and/or interfaces whose traffic needs to be analyzed.

Under Report Criteria, you can specify a maximum of three filtering criteria:

- Source/Destination Address
- Source/Destination Network
- Source/Destination Nodes
- Application
- Port/Port Range

The **From** and **To** boxes let you choose custom time periods for the report. Use the  icon to select the date and time easily. Use the **IN/OUT** box to display values based on IN traffic, OUT traffic, or both IN and OUT traffic. The **Show** box lets you choose how many results to display. You can set this value from the Settings page.

Once you select all the desired criteria, click the **Generate Report** button to display the corresponding traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values. You can also choose to print this report by clicking the  icon or the **Print** link.

	Custom Reports are different from Troubleshooting Reports. You can troubleshoot only one interface at a time, whereas Custom Reports can be generated across interfaces. Data for Troubleshooting reports is taken directly from raw data, whose maximum retention period can be set from Settings. But data for Custom Reports is taken from aggregated data in the database.

Admin Operations

Product Settings

The Settings option includes several server configuration settings that you can configure from the user interface namely :

- Server Settings
- Advanced Settings
- Storage Settings
- Google Map Settings

You can access these settings from OpManager, Admin-> Port Settings.

Server Settings

Server Settings

The Server Settings option includes several configuration settings that you can configure from the user interface. To configure the Server settings, from OpManager go to Admin-> Port Settings.

Option	Default Value	Requires server restart	Description
NetFlow / sFlow Listener Port	9996	yes	The port on which NetFlow Analyzer listens for NetFlow exports. You need to configure devices to send NetFlow exports to this port. In case you are exporting NetFlow from multiple routers, please configure multiple listener ports. You can specify upto 5 listener ports, each seperated by a comma. You will need to restart the NetFlow Analyzer server when you change the listener port
Webserver Port	8080	yes	The port used to access NetFlow Analyzer from a web browser
Record Count	100	no	This number governs the top N conversations that are retained for every 10 minute interval for each interface. Set it to 100 for maximum visibility into your traffic.The default record count is 100 but the minimum number of records that can be kept in the database for all traffic data is 10. This is also the maximum value that can be selected from the Show box in all traffic reports

DNS Settings

Option	Description
Resolving DNS Names	DNS names may be resolved only when "Resolve DNS"is clicked or automatically by default
DNS count in cache	The DNS count could take any value from 5000, 7500 and 10,000
User Defined DNS names	User defined DNS names can be entered or modified. This value will over-ride the system resolved DNS value.
Clear DNS Cache	Clicking on this button will clear all DNS entries that have been resolved by the system. The application asks for a confirmation before initating the clearing action

Advanced Settings

The Advanced Settings option includes the Flow Filter Settings and its corresponding configuration settings. To configure the Advanced settings, from OpManager go to Admin-> Port Settings-> Advanced Settings.

Flow Filter Settings

The Flow Filter settings empower the administrator with the option to

- exclude ESP_App on user defined interfaces - This helps in ensuring that traffic is not double counted in case of ESP tunnels.
- suppress Access Control List related drops (based on destination interface being null) on user defined interfaces.
- suppress output interface accounting on user defined interfaces - Useful when working with WAN accelarators

Option	Description
Select edge interfaces of a cryptomap tunnel to apply ESP application filter	One could add or modify interfaces to apply the ESP application filter. Enabling NetFlow on cryptomap tunnel interfaces double counts the ESP traffic. To prevent this please apply this filter on cryptomap tunnel interfaces. It is possible to add or modify interfaces.
Select interfaces to apply access control traffic filter	Access control filter drops the flow information which contains data pertaining to dropped traffic due to Access Control List. Please apply this filter to drop such flows. These flows have the destination interface as null. If any interface is selected to apply this filter, all the traffic coming from this interface with destination as null interface will be dropped.
Select interfaces to apply output interface suppression filter	Please select any WAN optimizer's LAN facing interfaces to suppress the incorrect out traffic (due to compression) reported by them. This filter stops the out traffic for any interface that is coming as a destination interface of a flow for a selected interface. When a WAN optimizer sends a flow which has source and destination interfaces as A and B respectively , if you select interface A to perform output suppression, B will not get out traffic which is not a correct traffic if reported by interface A (since compression is happening on interface B on the WAN optimizer)

Storage Settings

To configure the Storage settings, from OpManager go to Admin-> Port Settings-> Storage Settings.

NetFlow Raw Data Settings

NetFlow Analyzer classifies data into 2 types namely Aggregated Data and the Raw Data.

Aggregated Data represents the total IN and OUT traffic, the top 100 application and the top 100 conversation for each interface for every 10 minute intervals. Data is progressively stored in 10 minute, 1 hour, 6 hour, 24 hour and weekly data points for older data - the most recent data is available with 10 minute granularity and data older than 90 days is available in weekly granularity.

This mechanism of storing the top 100 is done to ensure that the database does not grow infinitely. The amount of hard disk space required to store the aggregated data forever is about 150 MB per interface.

In addition to the aggregated data, NetFlow Analyzer 5 allows you to store all raw netflow data for up to 1 month. The time period for which you can store this raw data (Raw Data Period) depends on the number of flows received by NetFlow Analyzer and the amount of free disk space available on your computer. Each flow is about 60 bytes. Troubleshooting and Alert reports are generated from Raw data since it provides high level of granularity.

NetFlow Analyzer indicates the flows received per second in the Raw Data Settings tab on the Settings link. You should set the raw data period (**Retain Raw Data**) based on the calculation below:

$$\text{Raw Data Period (in hours)} = \frac{\text{Free hard disk space - (150 MB * No. of Managed Interfaces)}}{\text{60 Bytes * 3600 seconds * Flows Per Second}}$$

You can use the recommendation provided by the software to set your Raw data storage period. The maximum raw data storage period is 1 month and the minimum is a day. Similar to the alerting feature, you can choose to have a mail sent whenever the disk space is less than a threshold value(This is set as a percentage value). In addition you can specify the free disk space threshold below which old raw data will be cleared up. This could be as percentage value of the total disk space. This can also take on the value of "Never", in which case the disk place is not cleared up at all.

One minute Data-Storage Settings

To set the period for which one minute flow data has to be stored use the **Retain One Minute Data** option. You could choose one of 1 month, 3 months, 6 months or 1 year. You will require a free disk space of 2MB to store one month of one minute traffic data for a single interface. The default period is 3 Months.

NBAR / CBQoS Data-Storage Settings

You can use this option to specify the time period for which NBAR data has to be retained. You could retain the NBAR data a minimum of 1 day or a maximum of 1 year. You will require a free disk space of 30 MB in order to store NBAR data for a month for each interface. The default value is 2 months.

Click on the "Update" button for the settings to take effect.

Google Map Settings

Google maps feature lets you physically locate your network resources on a map. This enables network administrators to have a feel of how distributed their network is and more importantly for quick and easier drill down to resource-specific information. Information on up to 3 top interfaces linked to a router is shown in the map. The Google Map settings lists all the devices and their corresponding location.This page gives you the option to place each of the devices in their respective locations

To access the Google Map settings, from OpManager go to Admin-> Port Settings-> Google Map Settings.

Assigning a location to a router

Clicking on the **Assign** link opens up the Google map. Follow the instructions below to place a device on the map:

1. Click on the location to place the device on the map. Use the controls on the top left to navigate or zoom
2. You will see an image indicating your selection
3. To change the location click on the image, it will vanish and then select a new location
4. Enter the location in the 'Location Name' field and hit "Save location"

Now a location has been assigned to a router.

Editing a location

To edit a specific location on the map, click on the "Edit" link under the Google Map Settings tab. Now the map view will open up with the location you had last specified.

To edit it (to move the pointer to the desired location) click on the area of the map where you think it should point to. The last location you spot(click) in the course of locating your resource through "n" different clicks on the map is taken as the final.

Deleting a location

You may remove any resource/ router from being shown on the map by clicking on the delete button against the resource in the Google Map Settings tab.

Application Mapping, Application Group, DSCP Mapping and DSCP Group

Application Mapping

The **Application Mapping** option lets you configure the applications identified by NetFlow Analyzer. You can add new applications, modify existing ones, or delete them from OpManager. Please see the Additional Notes on Application Mapping section to understand this feature more clearly. Also it is possible to associate an IP address with an application.

Adding an Application

Follow the steps below to add a new application:

1. From OpManager, go to Admin-> Application/QoS Mapping-> Application Mapping.
2. Click the **Add** button to add a new application
3. Enter the port number of the new application. To enter a port range, separate the start and end points of the range with a hyphen. (eg.) 1400-1700
4. Choose the protocol from the list of protocols
5. Choose one of the options from IP Address / IP Network / IP Range. Depending on what you opt a set of fields are enabled and should be filled.
    - If you opt for **IP Address** then you have to enter the address in the IP Address box.
    - If you opt for **IP Network** then you have to enter the IP Network and IP Netmask details.
    - If you opt for **IP Range** then you have to enter the Start IP, End IP and IP Netmask Enter a unique name for the application
6. The Application Name has to be entered finally by which the IP address is associated with an application.

	Ensure that the combination of port number and protocol is unique. If not, the older application mapping will be deleted.

Once you are done, click the **Update** button to save your changes.

Modifying an Application

Select an application and click the **Modify** button to modify its properties

	You can only change the name of the application. If you need to change the port or the protocol, you have to delete the application, and add it as a new application.

Once you are done, click the **Update** button to save your changes.

Deleting an Application

Select an application and click the **Delete** button to delete it. The application is permanently deleted, the corresponding port is freed, and can be assigned to another application

Additional Notes on Application Mapping

Applications are categorized based on the source address, destination address, source port, destination port and protocol values in the flow record. These values are matched with the list of applications in the Application Mapping.

The check is done first with the smaller of the 2 ports (source port / destination port), and if no match is found the bigger of the 2 ports is mapped

Application mappings created with specific IP address / IP Range / IP Network is given higher priority over applications mappings with no IP address. For example assume you have 2 application mappings as below:

Port	Protocol	IP Address / IP Range	Application
80	TCP	10.10.1.0(255.255.255.0)	APP1
80	TCP	Any	APP2

|f a flow is received with source address 10.10.10.10 and Port as TCP-80 then it is classified as APP1. Only TCP-80 flows from non-10.10.10.0 network will be classified as APP2.

Application mappings created with single port is given higher priority over applications mappings with port range. For example assume you have application mappings as below:

Port	Protocol	IP Address / IP Range	Application
80	TCP	any	APP1
70 - to - 90	TCP	any	APP2

If a flow is received with Port as TCP-80 then it is classified as APP1.

Applications are categorized based on the source address, destination address, source port, destination port and protocol values in the flow record.

The smaller of the 2 ports (source port / destination port) and protocol is matched with the port-protocol in the application mapping list

If no match is found, the bigger of the 2 ports (source port / destination port) and protocol is matched with the port-protocol in the application mapping list.

If no match is found, the smaller of the 2 ports (source port / destination port) and protocol is matched with the port range-protocol in the application mapping list.

If no match is found, the bigger of the 2 ports (source port / destination port) and protocol is matched with the port range-protocol in the application mapping list.

If no match is found, the application is categorized as protocol_App (as in TCP_App or UDP_App)

In case the protocol is not available in the application mapping list, the application is categorized as Unknown_App

The sequence in which the mappings are checked is as follows:

1. Application mapping with specific IP address / IP Range / IP Network is matched.
2. Application mapping with no IP address and single port number / port range.

Application Group

Application Groups allow you to define your own class of applications by including one or more applications. For example, you might want to classify all your database applications like Oracle, MySql, MS-Sql in to one group called the DataBase group. Initially when no application groups have been created a message to that effect is displayed. The Application Group report can be viewed on the Application tab for each interface.

Adding an Application Group

Follow the steps below to add a new application group:

1. From OpManager, go to Admin-> Application/QoS Mapping-> Application Group.
2. Click the **Add** button to proceed to the Add Group Screen
3. Enter the Group Name and the Group Description (eg.) DataBase Group - Contains the Oracle DB and MySql DB
4. Choose the applications from the list of applications in the left pane
    - Select an application by clicking on it.
    - Use the " >> " button to include the selected application to the right pane - "Selected Applications" list.
    - Add as many applications as you want to this group.
5. Click on update for the application group to be created with the list of applications you had selected.

You may create additional Application Groups by clicking on the Add button and following the above steps.

Modifying an Application Group

Select the Application Group you wish to modify and click on the "Modify" button.

You can only change the Application Group description and the list of selected applications. It is not possible to change the application group name.

Once you are done, click the **Save** button to save your changes.

Deleting an Application Group

Select the application group you want to delete and click on the "Delete" button. You are asked for a confirmation to delete and if you confirm the group is deleted.

DSCP Mapping

The DiffServ model for DSCP Mapping was developed to differentiate IP traffic so that the traffic's relative priority could be determined on a per-hop basis. Using DSCP Mapping you can name the DiffServ code points and monitor their traffic in troubleshooting reports under the DSCP tab. Note that the DSCP reports can be viewed on the Troubleshooting page by clicking on the DSCP tab.

Adding a new DSCP Mapping

From OpManager, go to Admin-> Application/QoS Mapping-> DSCP Mapping. Click on the Add button to create a new DSCP Mapping. A window pops out where you may enter the Group Name and the Code Point (a six-digit Binary Number). *For Example*: Data Centre devices - 001001. Click on the "Add" button to add this mapping.

Modifying a DSCP Mapping

Please note that it is not possible to modify a DSCP Mapping.

Deleting a DSCP Mapping

Select the DSCP Mapping (the combination of QoS Group Name and Code Points) you want to delete and click on the Delete button.

DSCP Group

Quality of Service is used to measure, improve and guarantee transmission rates, error rates and other characteristics in a networkes setting. The DiffServ model for DSCP Mapping was developed to differentiate IP traffic so that the traffic's relative priority could be determined on a per-hop basis. Using DSCP Mapping you can name the DiffServ code points and monitor their traffic in troubleshooting reports under the DSCP tab. Note that the DSCP reports can be viewed on the Troubleshooting page by clicking on the DSCP tab.The DCSP group is very valuable in the deployment of QoS.

Adding a new DSCP Group

Follow the steps below to add a new application group:

1. From OpManager, go to Admin-> Application/QoS Mapping-> DSCP Group.
2. Click the **Add** button to proceed to the Add Group Screen
3. Enter the Group Name and the Group Description (eg.) DataBase Group - Contains the Oracle DB and MySql DB
4. Choose the DSCP Names from the list of names in the left pane
    - Select a name by clicking on it.
    - Use the " >> " button to include the selected DSCP Name to the right pane - "Selected DSCP Names" list.
    - Add as many DSCP Names as you want to this group.
5. Click on Save for the DSCP Group to be created with the list of DSCP Names you had selected.

You may create additional DSCP Group by clicking on the Add button and following the above steps.

Modifying a DSCP Group

Select the DSCP Group you wish to modify and click on the "Modify" button.

You can only change the Group description and the list of selected applications. It is not possible to change the DSCP group name.

Once you are done, click the **Save** button to save your changes.

Deleting a DSCP Group

Select the DSCP Group you want to delete and click on the Delete button.

IP Group Management

The IP groups feature lets you monitor departmental, intranet or application traffic exclusively. You can create IP groups based on IP addresses and/or a combination of port and protocol. You can even choose to monitor traffic from specific interfaces across different routers. After creating an IP group, you can view the top applications, top protocols, top hosts, and top conversations in this IP group alone.

This section will help you understand IP Groups and walk you through the steps needed to create and later delete an IP group if needed.

Understanding IP Groups

To further understand how the IP grouping feature can help in understanding exclusive bandwidth usage, consider the following two scenarios:

Enterprise Network Scenario

A typical enterprise setup where the main servers and databases are located at a central office, and all branch offices are given appropriate access privileges to these servers.

> **Problem:** You need to track bandwidth used by each branch office while accessing an ERP/CRM application
> **Solution:** Create an IP group for each branch office, along with the port and protocol of the ERP/CRM application running in the central office.
>
> The traffic reports for each IP group will then show details on bandwidth used by the branch office while working with the ERP/CRM application. This information is very useful during traffic accounting and usage-based billing.
>
> **End Note:** If the IP addresses in the branch offices are NATed (network address translated) by the web server, you can view overall bandwidth usage for the branch office, but not that of individual hosts within the IP group.

Campus Network Scenario

A typical campus network with several departments. Here IP addresses are usually not NATed by the web server.

> **Problem:** You need to analyze bandwidth used by each department
> **Solution:** Create an IP group for each department (IP address or address ranges), without specifying any port/protocol values.
> The traffic reports for each IP group will then show bandwidth usage by that department along with information on top talkers, and top conversations within that department.

Defining IP Groups

IP groups can be defined based on IP address and/or port-protocol combinations. In addition, you can filter IP group traffic based on interfaces. The following matrix shows the different combinations possible, along with a typical example usage for each combination.

Combination	IP Address	Port/Protocol	Interfaces
IP Address	View bandwidth details for a range of IP addresses.	View Web (80/TCP, 80/UDP) traffic details for a range of IP addresses.	View bandwidth details across multiple interfaces, for a range of IP addresses.
Port/Protocol	View Web (80/TCP, 80/UDP) traffic details for a range of IP addresses.	View Web (80/TCP, 80/UDP) traffic generated across the network	View Web (80/TCP, 80/UDP) traffic generated across multiple interfaces.
Interfaces	View bandwidth details across multiple interfaces, for a range of IP addresses.	View Web (80/TCP, 80/UDP) traffic generated across multiple interfaces.	[Not possible]

Creating an IP Group

The **IP Group Management** link in the **Admin Operations** box lets you create, modify, and delete IP groups. Click this link, and then click **Create** to create a new IP group. Fill in the following information and click **Add** to add the new IP group to the current list of IP groups.

Field	Description
IP Group Name	Enter a unique name to identify this IP group
IP Group Description	Enter descriptive information for this IP group to help other operators understand why it was created.
IP Group Based on	Select whether you want to define this IP group based on IP address or port-protocol combination. If you want to define the IP group based on both IP address and port-protocol, select both options.
Specify IP/IP Range/Network	Select the IP address, address range, or network that this IP group is based on. Use the Add More option to add additional specifications.
Include/Exclude	Include option includes the particular the IP address, address range, or network. Exclude option excludes the particular the IP address, address range, or network.
Associated Interfaces	If you need to filter this IP group further, based on devices or different interface combinations, click the "Select Devices" link and select the different devices and interfaces whose traffic needs to be included in this IP group.
IP Group Speed	Enter the interface speed (in bits per second) for calculating percentage of traffic for this IP group.

If you add a new combination of ports and protocol, a popup opens stating that this combination of ports and protocol has not been mapped to any application. Add the combination as a new application in the same popup, and click Update to update the Application Mapping list with the new application.

Managing IP Groups

Click the **IP Group Management** link in the **Admin Operations** box to view the list of IP groups created so far. The current status of the IP Group is also shown as Enabled or Disabled. Select the IP group that you want to modify, and click the **Modify** button to edit its settings. Once you are

done, click **Add** to save and activate the new changes. To change a IP group's status from Enabled to Disabled or vice-versa click on the current status of the IP Group. It is possible to Enable or

Disable all the IP Groups at once by using the "Enable All" and "Disable All" buttons.

To delete an IP group, select the IP group and click the **Delete** button. Deleting an IP group removes the IP group from the list of IP groups managed. All users assigned to this IP group will not see this IP group listed on their Dashboard.

Unmanaging an IP group will lead to bill generation for the particular IP group, IF that IP group has been selected for billing.

Bulk loading IP Groups

NetFlow Analyzer allows bulk loading of IP group using the XML file(ipGroup.xml) contained in the location: **AdventNet\ME\NetFlow\troubleshooting**. using this file it is possible to define multiple IP groups at once. A sample configuration code looks like:

```
<IPGroups ip_group_name="Engineering" ip_group_desc="description in detail"
ip_group_speed="1000000">
<GrpIPAddress addr_id="12.12.12.12" flag="include"/>
<GrpIPNetwork netmask_addr_id="255.255.255.0" network_addr_id="12.12.13.0" flag="include"/>
<GrpIPRange netmask_addr_id="255.255.255.0" start_addr_id="12.12.14.1"
end_addr_id="12.12.14.100" flag="exclude"/>
<ApplicationNames port="80" protocol="TCP"/>
<Selected_Devices>
<Router Router_Name="192.168.111.113">
<Interface interface_name="IfIndex1" />
<Interface interface_name="IfIndex3" />
</Router>
</Selected_Devices>
</IPGroups>
```

Within this configuration it is possible to have any number of **GrpIPAddress** or **GrpIPNetwork** or **GrpIPRange** or **ApplicationNames** with Inteface selection.

It is also possible to add specific criteria/exceptions to the group definition such as:

- configuring an IP group with just one network
- configuring an IP group with just one address
- configuring an IP group with just one range
- configuring an IP group with just port and protocol

The user has to ensure that an IP group with the same name does not already exist and that the IP group name does not exceed 50 characters.
If all the IP groups are loaded succesfully, you can see the message "All ipgroups are succesfully loaded" in the User Interface. If you try to load the same IP groups twice, you can see the message "Error in loading. IPGroup with name ':grp1' Already exists." in the User Interface. If there is no such file in the directory, you can see the message "NETFLOW_HOME\troubleshooting\ipGroup.xml is not found." in the User Interface.

After adding the IP group(s) it is possible to selectively include/exclude a IP Network/ IP Address/ IP Range from the user interface of the product.

Alert Profiles Management

An alert profile is created to set the thresholds for generating alerts. The parameters to be set for creating an alert profile are;

- **Interfaces/ IP Groups / Interface Group** - The list of interfaces/ IP Groups / Interface Group whose bandwidth utilization must be watched
- **Traffic pattern** - The traffic to be watched - In Traffic, Out Traffic or a Combination of both
- **Application / Port(s)** - You can watch the traffic through all the applications or from a particular application. Similarly, through a single port or a range of ports
- **Threshold Settings** - It has 3 settings namely % utilization, no. of times, and duration.
    - **% Utilization** - When the utilization exceeds this limit, it is noted
    - **No. of time** - The number of times the utilization can be allowed to exceed the threshold before an alert is raised
    - **Duration** - The time period within which, if the threshold is exceeded the specified number of times - an alert is created(generated)

Netflow Analyzer calculates the bandwidth utilization of the specified interfaces/ IP Groups / Interface Group every minute. If the utilization exceeds the threshold value, the time when it exceeded is noted. Subsequently when it exceeds, the corresponding times are noted. If the number of times the utilization exceeds the specified limit, in the specified time duration, an alert is generated. When an alert is generated, you can also send an email to one / more people or send an SNMP trap to a manager application.

The **Alert Profile Management** option lets you create new alert profiles and manage existing ones (Modify or Delete). The Alert Profiles page lists all existing alert profiles, along with the number of alerts generated for each profile. The application comes loaded with a preconfigured alert that can trigger an email alert when a link goes down or when there are no flows for more than 15 minutes.

The various columns displayed in the Alert Profiles page are described in the table below:

Column	Description
Name	The name of the alert profile when it was created. Click on the alert profile's name to see more information about the alert profile.
Description	Descriptive information entered for this alert profile to help other operators understand why it was created.
Category	The category defines, to what type of alert an alert profile belongs to. The pre-loaded and pre-configured "Link Down" alert belongs to the "Link Status" category. All other alerts created by the user fall under the "Utilization"category.
Status (Enabled/Disabled)	This lists whether an alert profile is currently enabled or disabled. Click the Enabled icon to disable an alert profile. When this is done, alerts will no longer be generated for that alert profile. Click the Disabled icon to enable the alert. The Link Status alert becomes enabled only after the mail server settings have been set.
Last Hour Alerts	Lists the number of alerts generated for this alert profile in the last one hour. Colors are used to represent the number of alerts generated with each severity level. Red - Critical, Orange - Major, Yellow - Warning, and White - All. Click on each color to see the list of alerts generated with that severity.
All Alerts	Lists the total number of alerts generated for this alert profile. Colors are used to represent the number of alerts generated with each severity level. Red - Critical, Orange - Major, Yellow - Warning, and White - All. Click on each color to see the list of alerts generated with that severity.
Clear	Click the icon to clear all alerts generated for this alert profile

Alerts List

The Alerts List is displayed when you click on any color against an alert profile in the Alert Profiles page, or from any link in the **Generated Alerts** box on the left pane. The list shows the alerts that were generated with the respective severity, along with the device that generated the alert, the time the alert was generated, and an option to view more details about the alert.

Click the **Details** link in the View column against an alert to view detailed information about the alert. The pop-up that opens up, shows the traffic graph outlining traffic values ten minutes before and after the alert was generated, along with details on top applications, sources, destinations, and conversations recorded during that time interval.

Link Down Alert

This is a preconfigured alert to send an email when the link goes down or when there are no flows for more than 15 minutes. By default this profile is disabled. This is similar to other alerts that are manually configured except that it can't be deleted. It is possible to have emails sent by this alert whenever no flows are received for over 15 minutes. It becomes activated only after the mail server settings are configured.

Operations on Alert Profiles

You can create new alert profiles, modify, or delete existing ones from the Alert Profiles page.

Creating a new Alert Profile

Remember to set the `active timeout` value on the router to 1 minute so that alerts are generated correctly. Refer the Cisco commands section for more information on router settings.

The steps to create an Alert Profile are:

1. Login to the NetFlow Analyzer client and click "**Alert Profile Management**" under "**Admin Operations**" in the left panel
2. Click "**Add**" to add a new Alert Profile
3. Fill in the following details

Field	Description
Alert Profile Name	Enter a unique name to identify this alert profile
Description	Enter descriptive information for this alert profile to help other operators understand why it was created.
Select Source	By default all Interfaces / IP Groups/ Interface Group sending NetFlow exports are selected. If you want this alert profile to apply to certain interfaces/ ip groups / Interface Groups only, click the Modify Selection link. In the pop-up window, select the required devices and interfaces or select the IP Group Names and click Update to save your changes.
Define Alert Criteria	Select whether alerts need to be generated based on incoming traffic, outgoing traffic, or both. The default setting is for both(combined).
	Then select the application / port for which the alert has to be generated. This criteria can be very general - Any application traffic can be profiled - or it can be highly specific - Generate the alert only when a specific application, protocol, and/or port is used. To identify the overall link utilization the "No Criteria" option has to be chosen

Field	Description
Define Threshold and Action	Enter the threshold conditions (threshold utilization, no. of times it can exceed and the time duration) exceeding which the alert will be generated. You can also specify an action to be taken during the alert creation. - Email - to send a notification to one or more people. - SNMP Trap - to send a trap to the manager application (specify the <server name>:<port>:<community>). To add more threshold values, click 'Add Row' and add values

4. **Customizing from address**:You can customize the "From Address" from the mail server settings in Settings page.
5. After setting the required thresholds, click '**Save**'

The new alert profile is created and activated. The system watches the utilization and raises alarms when the specified conditions are met.

Only one alert is generated for a specified time duration. For example, say for a particular interface, the threshold is set as 60% and number of times is set as 3 times and the time duration is set as 30 minutes. Now lets assume that the utilization in that interface goes above 60% and stays above it. Then in 3 minutes, the above conditions will be met and an alert will be generated. The next alert will NOT be generated after 6 minutes, but only in the 33rd minute, if the condition persists. Thus for the specified 30 minutes time duration, only one alarm is generated. This is designed to avoid a lot of repetitive mail traffic.

Modifying or Deleting Alert Profiles

Select an alert profile, and click on **Modify** to modify its settings. You can change all of the alert profile's settings except the profile name. However, it is possible to modify the "Link Down" alert profile's name. There is also an option to clear details of all alerts created for this profile from this page itself. Once you are done, click **Save** to save your changes.

Select an alert profile, and click on **Delete** to delete the profile. Once an alert profile is deleted, all alerts associated with that profile are automatically cleared. However it is not possible to delete the "Link Down" alert profile.

Schedule Reports

 It is a good idea to schedule reports to be run at non-peak traffic hours since generation of reports is a resource hungry process especially for large interface numbers. A Scheduler is configured to set the parameters for automating the generation of reports. The parameters to be set for creating a Scheduler are:

- **Source -** The Interfaces or IP Groups which are the source of traffic.
  - **Interfaces** - The list of interfaces who's bandwidth utilization must be watched. One report will be generated for each interface selected
  - **IP Groups** - The IP groups who's bandwidth utilization must be watched. One report will be generated for each IP Group created
- **Report Type** - The type of report to be generated - Consolidated or Custom (custom report option not available under "IP Groups")
- **Report Generation Schedule** - How and when the report is to be generated (e.g.) daily,weekly,monthly,or only once
  - **Generate report on** - This value determines the time when report is to the generated
  - **Generate report for** - This value determines the start and the end time for the report
- **Email Address** - This is the address to which the generated reports will be sent

Netflow Analyzer calculates the bandwidth utilization on the specified interfaces / IP Groups every minute. Based on the schedule opted for, reports are generated at various time intrevals.The **Schedule Reports** feature lets you Create new Schedules and Delete existing ones. The Scheduler List page lists all existing schedules , along with the Schedule details,Status, Report types,and the Last Report Generated time.

The various columns displayed in the Scheduler List page are described in the table below:

Column	Description
Name	The name of the Schedule when it was created. Click on the Schedule's name to see more information about the schedule's configuration
Schedule Details	Information on when the schedule will run
Status	By default all schedules are Enabled, which means they are active. Click the Enabled icon to disable a schedule. When this is done, reports will no longer be generated for that configuration. Click the Disabled icon to enable the schedule again
Report Type	Whether it is a consolidated report are user-defined Custom report
Last Report Time	This column lists the last time when this schedule was run and a report created
Generated Reports	By clicking on View Reports it is possible to view all the previous reports that have been generated. The number of reports that are stored is based on the user definition in the Schedule Setting page. (By enabling the item "Enable older reports to be accessed from UI" it is possible to retrieve even older reports.) For Daily Schedule up to 90 reports can be stored. For Weekly Schedule up to 104 reports can be stored. For Monthly Schedule up to 60 reports can be stored.

Operations on Schedule Reports

You can create new schedules or delete existing ones from the Schedule List page.

Configuring a new Schedule

The steps to configure a Schedule are:

1. Login to the NetFlow Analyzer client and click "**Schedule Reports"** under "**Admin Operations**" in the left panel
2. Click "**Add**" to add a new Schedule Profile
3. Fill in the following details

Field	Description
Scheduler Name	Enter a unique name to identify this scheduler.
Description	Enter descriptive information for this scheduler profile to help other operators understand why it was created.
Select Source	By default all managed interfaces sending NetFlow exports are selected. If you want this schedule configuration to apply to certain interfaces only, click the Modify Selection link. In the pop-up window, select the required devices and interfaces and click Update to save your changes.
	By default all IP Groups are selected. If you want this schedule configuration to apply to certain IP Groups only, click the Modify Selection link. In the pop-up window, select the required devices and IP Groups and click Update to save your changes.
Report Type	Select whether the reports that need to be generated is consolidated or a customized one .The default setting is Consolidated Report.To opt for Custom Report click on the radio button in front of custom report.
	If you want a customized report then click on the radio button in front of custom report. Opting for Custom report lets you set criteria by using the "Add Criteria" option.Any number of criterion can be set and the rule set to match all the criteria or anyone.
Schedule Report Generation	Select the report generation frequency as one from : Daily, Weekly, Monthly and Only Once. Depending on this the report will be generated at the appropriate time intervals.
Email Address to Send Reports	Enter the email address to which the generated reports have to be emailed. You can enter multiple email addresses separated by a comma.

4. After setting the required parameters, click '**Save**'

Custom Report :

Opting for custom report lets you set criteria on the basis of which the report will be generated. By clicking on the "**Add Criteria**" button one can set a matching condition on "Source Address, Source Network, Source Nodes, Destination Address, Destination Network, Destination Nodes and Application". To add more criteria click on "**Add Criteria**" again. Having created all the criterions you can decide whether to make the generated report to match all of the criterions created or any of them.

Scheduling Report Generation

The report generation schedule can be chosen from one of the following:

- **Daily** - When you opt for "Daily" you have the option to set the time at which the report should be generated. Also, the report could be generated for the previous day or the last 24 hours. When the "Previous Day" option is opted the report is generated for the time period from 00:00 hours to 23:59 hours of the previous day. You have the option to narrow down this time

period by using the time filter -  . For instance if the maximum flow happens during your working hours from 08:00 hours to 18:00 hours you can set it in the window that pops up.

When you opt for the last 24 hours then the report is generated for the flow in the intervening 24 hours (from the time at which the report is to be generated today). The 30 most recent reports for this schedule can be accessible from the Schedule List page

Exclude weekends:

When you choose the Exclude Weekend option with "Previous day", reports will be generated on Tuesday, Wednesday, Thursday, Friday and Saturday. These will be reports pertaining to Monday, Tuesday, Wednesday, Thursday and Friday respectively.

When you choose the Exclude Weekend option with "Last 24 hours", reports will be generated on Monday, Tuesday, Wednesday, Thursday and Friday.

- **Weekly** - When you opt for the "Weekly" option, you have the option to specify the day and time at which the report needs to be generated. The report could be generated for the "Previous Week" or for the "Last 7 Days". By additionally opting for the "Exclude Weekend" the report can be made to include only data corresponding to monday through friday.

  The previous week option would generate the report for the time period Sunday 00:00 hours till Saturday 23:59 hours. When"Exclude Weekends" is enabled the report will be generated for the time period Monday 00:00 hours till Friday 23:59 hours.

  The"Last 7 Days" option would generate the report for the last 7 days from the time at which the report is to be generated. Again, the exclude weekend option would generate for the last 7 days with the data for the weekend (saturday,sunday) excluded. For instance if the report is to be generated at Monday 10:00 am, with the rules set as "last 7 days" and "Exclude weekend" enabled, then the report will be generated for the time period last week's Monday 10:00 hours to Friday 23:59 hours and from this week Monday's 00:00 hours till 10:00 hours. The 52 most recent reports for this schedule can be accessible from the Schedule List page

- **Monthly** - By opting for the "Monthly" option you can set the date of the month along with the time at which the report needs to be generated every month .The report could be generated for the "Previous Month" or for the "Last 30 days". By selecting "Exclude Weekends" the report can be made to include only data corresponding to monday through friday.

  When "Previous Month" option is enabled and the report generation date is set to 5-th of every month at 10:00 hours, then the report will be generated for the whole of last month (first to the last day of the month). When "Exclude weekend" option is enabled then the generated report will exclude all the intervening weekends (saturday & sunday).

  When "Last 30 Days" option is enabled and the report generation date is set to 5-th of every month at 10:00 hours, then the report will be generated from last month's 5-th 10:00 hours till this month 5-th's 10:00 hours. When"Exclude Weekend" option is enabled then the generated report will exclude all the intervening weekends(saturday & sunday). The 12 most recent reports for this schedule can be accessible from the Schedule List page.

- **Only Once** - If you wish to generate report only once at a specified time you can do that by opting for "Only Once". The date and time at which the report should be run can be specified. The date & time can be altered by using the icon -  . The report could be generated for the

Previous Day, Last 24 Hours, Previous Week, Last 7 Days, Previous Month, or Last 30 Days. When "Previous Day" option is enabled then the  button permits the setting of working hours. The latest report for this schedule can be accessible from the Schedule List page.

Customizing from address:

You can customize the "From Address" from the mail server settings in settings.

A note on emailed reports:

A report is generated for each interface / IP Group - 50 such reports are zipped in a single email and mailed. In case of more than 50 interface/ IP Groups selected the report will be sent in multiple emails. The last generated reports for all schedules will be under the folder NetFlow -> Reports.

Deleting Schedules

|elect a schedule from the Schedule List and click on **Delete** to delete the schedule. Once a schedule is deleted no longer reports are generated at the stipulated intervals. Deleting a schedule also deletes the corresponding folder.

Schedule Settings

In addition, there is the **Schedule Settings** link in the Schedule List Page. This link lets you set parameters that could be applied across all the generated reports. The parameters include:

- **Host Name display in reports -** This determines how the host name is displayed in reports. It could be chosen as one of
  - IpAddress (or)
  - DNS Name
- **Graph Options (**Report Type to be shown in reports**)** - This determines how the data is to be shown in the generated reports. This could be one of
  - Utilization (in %) (or)
  - Speed (in bps)
- **Report Mail-Attachment option** - The format in which the attachments are to be mailed. It could be one of
  - Zipped file (or)
  - PDF - The number of PDF files to be sent in a mail is to be specified. The number may range from 5 to 50 in increments of five
- **Enable older reports to be accessed from UI**
  - Daily Schedules - the number of daily reports to be stored (it can take values of 7 / 30 / 60 / 90)
  - Weekly Schedules - the number of weekly reports to be stored (it can take values of 4 / 26 / 52 / 104)
  - Monthly Schedules - the number of monthly reports to be stored (it can take values of 12 / 36 / 60)

Once the schedule settings have been configured, click on the "Save" button to apply this settings from hereon. Also click on "Close" button to close the window and proceed to the Schedule List page.

Device Group Management

NetFlow Analyzer lets you create device groups, which consist of a set of routers. A device group can contain any number of routers, and a router can belong to any number of device groups.

The **Device Group Management** option lets you create, manage, and delete device groups. Initially, when no device groups have been created, you will see a message that lets you start creating device groups.

	The options visible under the Admin Operations menu depend on the user level you have logged in as. Look up User Management to know more about user levels and the respective administrative operations allowed.

Creating a Device Group

Follow the steps below to create a new device group:

1. Click the **Add** button to create a new device group
2. Enter a unique name to identify the device group. The same name is displayed in the Device Group menu on the left, and will be listed under Available device groups when managing a user.
3. Use the **Device Group Description** box to enter useful information about the device group
4. Select the routers needed for this device group from the list of available routers displayed

Once all values have been entered, click the **Update** button to create this device group and begin generating traffic reports for the same.

Managing a Device Group

Select an existing device group and click the **Modify** button to modify its properties. You can change all properties of the device group except its name. Once you have made changes to the properties of this device group, click the **Update** button to save your changes.

Select an existing device group and click the **Copy** button to copy its settings. This is useful when you need to create a new device group that includes the same routers as that of this device group. This saves you the trouble of adding the routers all over again. Then follow the same steps as those in creating a new device group.

Select a device group and click the **Delete** button to delete the device group. When a device group is deleted, it is removed from the Device Group List and the Device Group menu. All users assigned to this device group will not see this device group on their Dashboard.

Interface Group

Interface Group allows you to combine interfaces in order to monitor traffic. This can be useful for grouping multiple sub-interfaces into a single logical entity.Follow the steps below to create a new interface group:

1. Click the **Interface Group** tab next to the Device Group tab
2. Enter a name to identify the interface group in the **Interface Group Name** box .

3. Use the **Interface group speed** box to enter the speed limit for the interface group
4. Select the routers needed and the interfaces under them for this interface group. By selecting a router ,by default, all interfaces are selected. You can selectively unselect the unwanted interfaces from the list.
5. Click on **Add** to save the changes.

The Interface group that is created is listed in the Dashboard view in the "Interface View" tab.The Interface group name, the In-Traffic & Out-Traffic for the last 1 hour can be seen in it.By clicking on the interface group name it is possible to further drill down to view further details. To delete a particular interface group select the interface group and click on delete.

Billing

Billing feature helps you keep a tab on resource usage and takes the bandwidth monitoring one step ahead - Accounting. It makes easy to understand the reports in terms of cost incurred. Internally, organizations can use this feature for department-wise billing. Also Internet Service Providers can use this to automatically generate reports for their customers.

Operations on Billing

Billing can be accessed from NetFlow, under **Admin Operations.**

Creating a Bill Plan

The **"Bill Plan List"** tab lets you create a new bill plan. To create a bill plan, click on the **"Add Plan"** tab. The Fields and their description are given below.

Enter Billing Details

Field	Description
Bill Plan	Enter the name you wish to assign for this bill plan
Bill Plan Description*	Describe the plan for detailed understanding and for future reference
Base Speed	Enter the base speed of the connection in bps (bits per second)
Base Cost	Select the currency from the drop-down box and enter the cost
Additional Speed*	Enter the additional speed of the connection in bps
Additional Cost*	Enter the cost for additional usage
95th Percentile Calculation	Select one of the two options from the drop-down box. Selecting "In & Out merge" will merge the In and Out values and calculate the 95 percentile value. Selecting "In & Out separate" will calculate 95th percentile value of IN and 95th percentile value of OUT separately and the higher of the two is considered. This is calculated using 5 minutes average data points. For better understanding, see the example.
Billing Period	Lets you select the option as quarterly or monthly. Incase you select the billing plan as quarterly, the bill will be generated quartely on the dateyou specify in the "Bill generation date" option. Incase you select the billing plan as monthly, the bill will be generated on a monthly basis on the date you specify in the "Bill generation date" option.
Bill Generation Date	Enter the date on which you want the bill to be generated either on monthly basis or quartely basis.

* - optional fields. Other fields are mandatory.

Associated To

This has the list of Routers/interfaces and IP groups. You can select the interfaces and/or the IP groups that is associated with this plan.

Once an Interface/IP Group is added to one bill plan, the specific interface/IP Groups does not get displayed while creating other bill plans

Email ID To Send Reports

Enter the mail ID/IDs to which the generated Bill report needs to be sent. Multiple mail IDs should be separated by comma ","

Example for the 95th Percentile calculation:

IN & OUT MERGE:

inbound = [0.139 0.653 0.201 0.116 0.084 0.032 0.047 0.185 0.198 0.203 0.276 0.370 0.971 0.233 0.218 0.182 0.169 0.126 0.131 0.157**]**
outbound = [1.347 1.435 1.229 0.523 0.438 0.231 0.347 0.689 0.940 1.248 1.385 1.427 3.988 1.265 1.221 1.013 0.992 0.874 0.896 1.002**]**

Inbound and Outbound merge

= [0.139 0.653 0.201 0.116 0.084 0.032 0.047 0.185 0.198 0.203 0.276 0.370 0.971 0.233 0.218 0.182 0.169 0.126 0.131 0.157 1.347 1.435 1.229 0.523 0.438 0.231 0.347 0.689 0.940 1.248 1.385 1.427 3.988 1.265 1.221 1.013 0.992 0.874 0.896 1.002**]**

> **Sorted_In & Out= [**3.988 1.435 1.427 1.385 1.347 1.265 1.248 1.229 1.221 1.013 1.002 0.992 0.971 0.940 0.896 0.874 0.689 0.653 0.523 0.438 0.370 0.347 0.231 0.276 0.233 0.218 0.203 0.201 0.198 0.185 0.182 0.169 0.157 0.139 0.131 0.126 0.116 0.084 0.047 0.032**]**
>
> Sorted In and Out contains set contains 40 samples--5% of 40 is 2, so discarding the top 5% means we must discard the top two samples from the data set. We are now left with:
>
> **Sorted_In & Out= [**1.427 1.385 1.347 1.265 1.248 1.229 1.221 1.013 1.002 0.992 0.971 0.940 0.896 0.874 0.689 0.653 0.523 0.438 0.370 0.347 0.231 0.276 0.233 0.218 0.203 0.201 0.198 0.185 0.182 0.169 0.157 0.139 0.131 0.126 0.116 0.084 0.047 0.032**]**
>
> The highest sample from remaining data set is the 95th percentile value for the originating set. So we obtain the following value:
>
> **95th_in & out** = **1.427 Mbps**

IN & OUT SEPERATE:

> **inbound = [**0.139 0.653 0.201 0.116 0.084 0.032 0.047 0.185 0.198 0.203 0.276 0.370 0.971 0.233 0.218 0.182 0.169 0.126 0.131 0.157**]**
>
> **outbound = [**1.347 1.435 1.229 0.523 0.438 0.231 0.347 0.689 0.940 1.248 1.385 1.427 3.988 1.265 1.221 1.013 0.992 0.874 0.896 1.002**]**

After sorting, we obtain:

> **sorted_in = [**0.971 0.653 0.370 0.276 0.233 0.218 0.203 0.201 0.198 0.185 0.182 0.169 0.157 0.139 0.131 0.126 0.116 0.084 0.047 0.032**]**
>
> **sorted_out = [**3.988 1.435 1.427 1.385 1.347 1.265 1.248 1.229 1.221 1.013 1.002 0.992 0.940 0.896 0.874 0.689 0.523 0.438 0.347 0.231**]**

Each sample set contains 20 samples--5% of 20 is 1, so discarding the top 5% means we must discard the top sample from each data set. We are now left with:

remaining_in = [0.653 0.370 0.276 0.233 0.218 0.203 0.201 0.198 0.185 0.182 0.169 0.157 0.139 0.131 0.126 0.116 0.084 0.047 0.032**]**

remaining_out = [1.435 1.427 1.385 1.347 1.265 1.248 1.229 1.221 1.013 1.002 0.992 0.940 0.896 0.874 0.689 0.523 0.438 0.347 0.231**]**

The highest sample from each remaining data set is the 95th percentile value for the originating set. So, for each set, above, we obtain the following values:

95th_in = 0.653 Mbps

95th_out = 1.435 Mbps

The higher of the two computed 95th percentile values becomes the final 95th percentile value used for billing:

95th percentile = 1.435 Mbps

Editing Bill Plan

Bill plans can be edited by clicking Bill plans list and editing any particular bill as the need may be.

Adding an interface/IP group

An interface/IP group can be added during any point of the billing cycle. The bill will be generated for this interface/IP group during the mentioned billing date for the billing plan.

Removing an interface/IP group

When an Intereface/IP group is removed from a bill plan, the bill for that interface is generated at the same instant.

	"Billing period" and "Bill generation date" CANNOT be changed. When the interfaces/ IP groups are unmanaged/ deleted, bill is generated for the interface or IP groups at that instant. If you modify the cost in the bill plan, It will be effected from the next billing cycle and NOT at that instant.

Deleting Bill Plan

Deleting a bill plan will lead to deletions of all the reports generated by the particular bill plan.

Reports

Generated Reports can be viewed by clicking the **"Report"** tab on top.

Available plans

You can view all the plans or any one plan by selecting the suitable option from the drop-down box. By default the "report" page shows only the recent report of all the bill plans. If you wan to view all the generated reports for a particular bill plane, select the bill plan from the dropdown box, next to "available plans". The reports are arranged with the most recent report on top.

Show details

By clicking on "show details" a pop up window opens, wherein you can view a speed-time graph.This shows all the bills generated for the particular interface.The report in can be generated in PDF format by clicking on **"PDF"** and you can view the data at 5 minutes interval by clicking on the **"Data points"**

NBAR

NBAR Reporting

What is NBAR?

NBAR (Network Based Application Recognition) is an intelligent classification engine in Cisco IOS Software that can recognize a wide variety of applications like Web-based and client/server applications. It can analyze & classify application traffic in real time. NBAR is supported in most Cisco switches and routers and this information is available via SNMP. Click here to view the list of protocols that are recognized by NBAR.

Why do I need NBAR?

NBAR, by adding intelligent network classification to your infrastructure, helps in ensuring that the network bandwidth is used efficiently by working with QoS(Quality Of Service) feature. With NBAR, network-traffic classification becomes possible and by this we can know how much of say , HTTP traffic is going on. By knowing this, QoS standards can be set. Unlike NetFlow, which relies on port & protocol for application categorization, NBAR performs a deep-packet inspection and allows you to recognize applications that use dynamic ports. Also, the NBAR approach is useful in dealing with malicious software using known ports to fake being "priority traffic", as well as non-standard applications using non-determinaly ports.

How do I enable NBAR?

You will first have to check whether your router supports NBAR. Please visit here to know about the Platforms & IOS that support NBAR. NBAR can be enabled only on those interfaces which are identified by NetFlow Analyzer.

If your router supports NBAR, then you will have to enable NBAR on each of the interface that you want to collect NBAR statistics.

NBAR can be enabled in two ways:

- Enabling on the device
- Enabling from the NetFlow Analyzer user interface

Enabling on the device

The following is a set of commands issued on a router to enable NBAR on the FastEthernet 0/1 interface.

```
router#enable
Password:*****
router#configure terminal
router-2621(config)#ip cef
router-2621(config)#interface FastEthernet 0/1
router-2621(config-if)#ip nbar protocol-discovery
router-2621(config-if)#exit
router-2621(config)#exit
router-2621(config)#show ip nbar protocol-discovery
```

 Please note that the part in red has to be repeated for each interface individually.

Enabling from NetFlow Analyzer User Interface

Alternately, you may check the router's NBAR supported status and also enable NBAR on the interfaces from the NetFlow Analyzer's NBAR Configuration page. The steps to enable from User Interface are:

1. Under **NBAR enabled interfaces** : You will first have to enable NBAR on an interface before you can start collecting NBAR data. This step allows you to enable NBAR on the interface. Enabling NBAR on the interface is done through SNMP and requires SNMP write community.

    1. Use the "Click Here" link to enable NBAR on Interfaces.
    2. Set SNMP Read Community, SNMP Write Community & the Port, in case you want to alter the default parameters. The values given during installation are prepopulated in the screen.
    3. Click on "Check Status" to see if the interfaces on the router have NBAR enabled on them. Click on "Check all Status" at the top of the window to know the NBAR support status of all the interfaces (under various routers). At the end of the status check a message is displayed at the bottom of the window(of each router pane). If NBAR has been enabled on the interfaces then the message " Success : NBAR status of the interfaces updated" is displayed. If the Check Status operation didnt succeed, due to SNMP error or Request Time-Out, then the message "SNMP Error : NBAR status of the interfaces not updated" is displayed. Also NBAR support is displayed as 'Yes' or 'Unknown' under the router name as the case may be.
        - In the right pane the status of each interface is shown under "NBAR Status". If NBAR is enabled on all interfaces then the status is shown as "Enabled" against each of the interfaces in that router.
    4. Select the interfaces you want NBAR to be enabled on(which are currently not enabled).
    5. Click on "Enable NBAR".
    6. If NBAR is enabled on the interface then the status will be displayed as "Enabled" against each of the selected interfaces. If NBAR cannot be enabled on the interface then the status will be displayed in red (Unknown or Disabled).

How do I disable NBAR?

Disabling NBAR can be done in two ways.

- Disabling on the device
- Disabling from the NetFlow Analyzer user interface

Disabling on the device

The following is a set of commands issued on a router to disable NBAR on the FastEthernet 0/1 interface.

```
router#enable
Password:*****
router#configure terminal
router-2621(config)#interface FastEthernet 0/1
router-2621(config-if)#no ip nbar protocol-discovery
router-2621(config-if)#exit
router-2621(config)#exit
```

 Please note that the part in red has to be repeated for each interface individually.

Disabling from NetFlow Analyzer User Interface

The steps to disable from User Interface are:

1. Under **NBAR enabled interfaces**: This step allows you to disable NBAR on the interface. Disabling NBAR on the device is done through SNMP and requires you to provide the SNMP write community.
    1. Click on "Modify Interfaces".
    2. Set SNMP Read Community, SNMP Write Community & the Port, in case it is not already set.
    3. Select the interfaces on which you want to disable NBAR and click on "**Disable NBAR**".
    4. If NBAR is disabled on the interface then the status will be displayed as "Disabled" against each of the selected interfaces. If NBAR cannot be disabled on the interface then the status will be displayed in red (Unknown or Enabled).

Polling

What is Polling - The process of sending the SNMP request periodically to the device to retrieve information (Traffic usage/ Interface Statistics in this case) is termed polling. A low polling interval (of say 5 minutes) gives you granular reports but may place an increased load on your server if you poll large amount of interfaces. Time out value needs to be set to a higher value in case your routers are at remote locations.
After NBAR has been enabled on select interfaces the polling can be started on those interfaces.

Start Polling

Polling can be done on those interfaces on which NBAR has been enabled earlier.Please do the following to start polling on an interface:

1. Under **"Polling for NBAR data"** :
    1. Use the link "click here " to invoke the screen which lists the NBAR enabled interfaces.
    2. Select the interfaces on which you want to do polling.
    3. Set the Polling Parameters - the Polling Interval & the Time Out. The Polling interval decides the frequency at which the NetFlow Analyzer server will poll the device. Time out is the amount of time for which NetFlow Analyzer server waits for the SNMP response from the device.
    4. Click "**Update**" to update the Polling Parameters.

Stop Polling

Polling can be stopped on those interfaces by following these steps.

1. Under **"Polling for NBAR data"** :
    1. Use the "Modify Poll Parameters" to invoke the screen, which lists the already polled interfaces with the check box selected and the "Polling Status" set as "Polling".
    2. Unselect the interfaces on which you want to stop polling.
    3. Click "**Update**" to stop polling.

The default NBAR data storage period is 2 months. You can change the storage period from Raw Data Settings under Settings page.

NBAR Report

The **NBAR Report** tab lists the various applications in your network and their percentage of the total traffic for the selected time period. The default view shows the **NBAR Application - In Report**. This report shows the distribution of traffic application-wise.

Choose between **IN** and **OUT** to display the application-wise distribution of incoming or outgoing traffic respectively.

The Time Period box lets you choose between last hour, last day, last week, last month, and last quarter's traffic graphs. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show** button to display the appropriate application traffic report.

The table below the graph shows the distribution of traffic per application. You can see what application caused how much traffic, and how much of the total bandwidth was occupied by that application.

Click the  icon (**Supported Applications** link) to see the list of supported applications, in a new window.

Viewing Top Applications

Choose between **IN** and **OUT** to display the protocol-wise distribution of incoming or outgoing traffic respectively.

The pie chart below shows what percentage of bandwidth is being used by each Application. The  icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can click the  icon to save the pie chart as a PDF file.

NBAR supported applications

NBAR supports a wide range of network protocols.The following list shows some of the supported protocols:

Peer-to-Peer Protocols

Peer-to-Peer Protocol	Type	Description
BitTorrent	TCP	File-sharing application
Gnutella	TCP	File-sharing application
Kazaa2	TCP	File-sharing application
eDonkey	TCP	File-sharing application
Fasttrack	TCP	File-sharing application
Napster	TCP	File-sharing application

VoIP Protocols

VoIP Protocol	Type	Description
SCCP	TCP	Skinny Call Control Protocol
SIP	TCP and UDP	Session Initiation Protocol
MGCP	TCP and UDP	Media Gateway Control Protocol
H.323	TCP and UDP	An ITU-T standard for digital videoconferencing over TCP/IP networks
SKYPE	TCP and UDP	Application allowing telephone conversation over the Internet

TCP & UDP stateful protocols

TCP or UDP Stateful Protocol	Type	Description
FTP	TCP	File Transfer Protocol
Exchange	TCP	MS-RPC for Exchange
HTTP	TCP	HTTP with URL, host, or MIME classification
Citrix	TCP	Citrix published application
Netshow	TCP/UDP	Microsoft Netshow
RealAudio	TCP/UDP	RealAudio Streaming Protocol
r-commands	TCP	rsh, rlogin, rexec
StreamWorks	UDP	Xing Technology Stream Works audio/video
SQL*NET	TCP/UDP	SQL*NET for Oracle
SunRPC	TCP/UDP	Sun Remote Procedure Call
TFTP	UDP	Trivial File Transfer Protocol
VDOLive	TCP/UDP	VDOLive streaming video

Non- TCP & Non-UDP protocols

Non-UDP or Non-TCP Protocol	Type	Well-Known Port Number	Description
EGP	IP	8	Exterior Gateway Protocol
GRE	IP	47	Generic Routing Encapsulation
ICMP	IP	1	Internet Control Message Protocol
IPINIP	IP	4	IP in IP
IPsec	IP	50, 51	IP Encapsulating Security Payload/Authentication Header
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol

TCP & UDP static port protocols

TCP or UDP Static Port Protocol	Type	Well-Known Port Number	Description
BGP	TCP/UDP	179	Border Gateway Protocol
CU-SeeMe	TCP/UDP	7648, 7649	Desktop videoconferencing
CU-SeeMe	UDP	24032	Desktop videoconferencing
DHCP/Bootp	UDP	67, 68	Dynamic Host Configuration Protocol/Bootstrap Protocol
DNS	TCP/UDP	53	Domain Name System
Finger	TCP	79	Finger User Information Protocol
Gopher	TCP/UDP	70	Internet Gopher Protocol
HTTP	TCP	80	Hypertext Transfer Protocol
HTTPS	TCP	443	Secured HTTP
IMAP	TCP/UDP	143, 220	Internet Message Access Protocol
IRC	TCP/UDP	194	Internet Relay Chat
Kerberos	TCP/UDP	88, 749	The Kerberos Network Authentication Service
L2TP	UDP	1701	L2F/L2TP Tunnel
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol
MS-SQLServer	TCP	1433	Microsoft SQL Servertop videoconferencing
NetBIOS	TCP	137, 139	NetBIOS over IP (Microsoft Windows)
NetBIOS	UDP	137, 138	NetBIOS over IP (Microsoft Windows)
NFS	TCP/UDP	2049	Network File System
NNTP	TCP/UDP	119	Network News Transfer Protocol
Notes	TCP/UDP	1352	Lotus Notes

TCP or UDP Static Port Protocol	Type	Well-Known Port Number	Description
NTP	TCP/UDP	123	Network Time Protocol
PCAnywhere	TCP	5631, 65301	Symantec PCAnywhere
PCAnywhere	UDP	22, 5632	Symantec PCAnywhere
POP3	TCP/UDP	110	Post Office Protocol
PPTP	TCP	1723	Point to Point Tunneling Protocol
RIP	UDP	520	Routing Information Protocol
RSVP	UDP	1698,1699	Resource Reservation Protocol
SFTP	TCP	990	Secure FTP
SHTTP	TCP	443	Secure HTTP
SIMAP	TCP/UDP	585, 993	Secure IMAP
SIRC	TCP/UDP	994	Secure IRC
SLDAP	TCP/UDP	636	Secure LDAP
SNNTP	TCP/UDP	563	Secure NNTP
SMTP	TCP	25	Simple Mail Transfer Protocol
SNMP	TCP/UDP	161, 162	Simple Network Management Protocol
SOCKS	TCP	1080	Firewall security protocol
SPOP3	TCP/UDP	995	Secure POP3
SSH	TCP	22	Secured Shell
STELNET	TCP	992	Secure TELNET
Syslog	UDP	514	System Logging Utility
Telnet	TCP	23	Telnet Protocol
X Windows	TCP	6000-6003	X11, X Windows

For more information click here

NBAR supported platforms & IOS Versions

Platforms & Cisco IOS Versions that currently support **CISCO-NBAR-PROTOCOL-DISCOVERY-MIB** are

- Cisco 1700 Series Router since Release 12.2(2)T
- Cisco 2600, 3600, 7100, 7200 Series Routers since Release 12.1(5)T
- Cisco 3700 and 7500 Series Routers since Release 12.2(8)T

The following Platforms also support NBAR:

- Cisco 800 Series Routers
- Cisco 1800 Series Integrated Services Routers
- Cisco 2600XM Series Router
- Cisco 2800 Series Integrated Services Routers
- Cisco 3700 Series Multiservice Access Routers
- Cisco 3800 Series Integrated Services Routers
- Cisco 7300 Series Routers
- Cisco 7400 Series Routers
- Catalyst 6500 Family Switch with a FlexWAN card.

To know the supported IOS versions check here

CBQoS

What is CBQoS ?

CBQoS (Class Based Quality of Service) is a Cisco feature set that is part of the IOS 12.4(4)T and above. This information is retreived using SNMP and provides information about the QoS policies applied and class based traffic patterns within an enterprise's network.

Why do I need CBQoS ?

Typically, networks operate on the basis of best-effort delivery, in which all traffic has equal priority and an equal chance of being delivered. When congestion results, all traffic has an equal chance of being dropped. QoS selects network traffic, prioritizes it according to its relative importance, and uses congestion avoidance to provide priority-indexed treatment; CBQoS can also limit the bandwidth used by network traffic. CBQoS can make network performance more predictable and bandwidth utilization more effective. Network administrators implement CBQoS policies to ensure that their business-critical applications receive the highest priority on the network. CBQoS provides you indepth visibility into the policies applied on your links and the traffic patterns in your various class of traffic. The pre-policy, post-policy and drops in different traffic class along with the queuing status enables you to validate the efficiency of your QoS settings.

Creating a traffic class
Creating a traffic policy
Attaching a Traffic Policy to an Interface
Verifying the Traffic Class and Traffic Policy Information

How do I start CBQoS data collection ?

Configuring Policies on the router

Initially CBQoS has to be enabled on the router manually. Further, policies have to be defined on the router. Usually, Traffic Policies are dependent on the type of the enterprise and its business needs.(heavy voice traffic, heavy document transfer, heavy streaming video traffic etc). The policy (classification) can be done on the basis of Class Maps and Policy Maps.

A class map is a mechanism that you use to isolate and name a specific traffic flow (or class) from all other traffic. The class map defines the criterion used to match against a specific traffic flow to further classify it; the criteria can include matching the access group defined by the ACL or matching a specific list of DSCP or IP precedence values. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. After a packet is matched against the class-map criteria, you can specify the QoS actions via a policy map. A policy map specifies the QoS actions for the traffic classes. Actions can include trusting the CoS or DSCP values in the traffic class; setting a specific DSCP or IP precedence value in the traffic class; or specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile. Before a policy map can be effective, you must attach it to an interface.

After a packet is classified and has an internal DSCP value assigned to it, the policing and marking process has to be done. Policing involves creating a policy that specifies the bandwidth limits for the traffic. Packets that exceed the limits are *out of profile* or *nonconforming*. Each policer specifies the action to take for packets that are in or out of profile. These actions, carried out by the marker, include passing through the packet without modification, dropping the packet, or marking down the packet with a new DSCP value that is obtained from the configurable policed-DSCP map.

Fetching Policy details from the router

Under the QoS Configuration tab the interfaces that have policies applied on them are displayed along with the router names and specific IN and OUT Policies. To facilitate the NetFlow Analyzer application to recognise the policies applied at each router level, click on the 

icon. This invokes a new window with the List of all routers, along with their Read Community & Port details. By clicking on "Check Status" or "Check All Status" it is possible to fetch the policy details from the router about each individual interface.

Once the policy details have been fetched from the routers the following message is displayed: "Policy Details Updated". If any policy is not found the the "Not Available" message is diaplayed.

Polling for CBQoS data

After setting the policies on the router and fetching the policy details polling can be started. Click on the "Modify Interfaces" button to select/unselect the interfaces on which polling has to be done. The Polling Parameters namely Polling Interval and Time Out can also be modified. The Polling interval can take any value from 5, 10, 15, 25, 30, 60. Time Out can take values from 5, 10, 15. After selecting/unselecting the list of interfaces on which Polling has to be done and after the Polling Parameters have been set click on "Update" to start the polling action.

Creating a traffic class

To create a traffic class, use the **class-map** command. The syntax of the **class-map** command is as follows:

class-map [**match-any** | **match-all**] *class-name*
no **class-map** [**match-any** | **match-all**] *class-name*
The match-all and match-any Keywords
The **match-all** and **match-any** keywords need to be specified only if more than one match criterion is configured in the traffic class.
The **match-all** keyword is used when *all* of the match criteria in the traffic class must be met in order for a packet to be placed in the specified traffic class.
The **match-any** keyword is used when only *one* of the match criterion in the traffic class must be met in order for a packet to be placed in the specified traffic class.
If neither the **match-all** nor **match-any** keyword is specified, the traffic class will behave in a manner consistent with **match-all** keyword.

About The match not Command

The **match not** command, rather than identifying the specific match parameter to use as a match criterion, is used to specify a match criterion that prevents a packet from being classified as a member of the class. For instance, if the **match not qos-group 6** command is issued while you configure the traffic class, QoS group 6 becomes the only QoS group value that is not considered a successful match criterion. All other QoS group values would be successful match criteria.

Procedure

To create a traffic class containing match criteria, use the **class-map** command to specify the traffic class name. Then use one or more **match** commands to specify the appropriate match criteria. Packets matching the criteria you specify are placed in the traffic class.

	In the following steps, a number of match commands are listed. The specific match commands available vary by platform and Cisco IOS release. For the match commands available, see the Cisco IOS command reference for the platform and Cisco IOS release you are using.

Configuration steps		
	Command or Action	**Purpose**
Step 1	Router> enable	Enables privileged EXEC mode.
Step 2	Router # configure terminal	Enters global configuration mode.
Step 3	Router(config)# class-map [match-all | match-any] class-name	Creates a class to be used with a class map, and enters class-map configuration mode. The class map is used for matching packets to the specified class. Note : The match-all keyword specifies that all match criteria must be met. The match-any keyword specifies that one of the match criterion must be met.
	Use one or more of the following match commands, as applicable.	
Step 4	Router(config-cmap)# match access-group {access-group | name access-group-name	(Optional) Configures the match criteria for a class map on the basis of the specified access control list (ACL). Note: Access lists configured with the optional log keyword of the access-list command are not supported when configuring a traffic class.
Step 5	Router(config-cmap)# match any	(Optional) Configures the match criteria for a class map to be successful match criteria for all packets.
Step 6	Router config-cmap)# match class-map class-name	(Optional) Specifies the name of a traffic class to be used as a matching criterion (for nesting traffic class [nested class maps] within one another).
Step 7	Router(config-cmap)# match cos cos-number	(Optional) Matches a packet based on a Layer 2 class of service (CoS) marking.
Step 8	Router(config-cmap)# match destination-address mac address	(Optional) Uses the destination Media Access Control (MAC) address as a match criterion.
Step 9	Router(config-cmap)# match discard-class class-number	(Optional) Matches packets of a certain discard class.
Step 10	Router(config-cmap)# match [ip] dscp dscp-value [dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value]	(Optional) Identifies a specific IP differentiated service code point (DSCP) value as a match criterion. Up to eight DSCP values can be included in one match statement.
Step 11	Router(config-cmap)# match field protocol protocol-field {eq [mask] | neq [mask] | gt | lt | range range | regex string} value [next next-protocol]	(Optional) Configures the match criteria for a class map on the basis of the fields defined in the protocol header description files (PHDFs).
Step 12	Router(config-cmap)# match fr-dlci dlci-number	(Optional) Specifies the Frame Relay data-link connection identifier (DLCI) number as a match criterion in a class map.
Step 13	Router(config-cmap)# match input-interface interface-name	(Optional) Configures a class map to use the specified input interface as a match criterion.
Step 14	Router(config-cmap)# match ip rtp starting-port-number port-range	(Optional) Configures a class map to use the Real-Time Protocol (RTP) protocol port as the match criterion.

Configuration steps		
	Command or Action	**Purpose**
Step 15	Router(config-cmap)# match mpls experimental mpls-values	(Optional) Configure a class map to use the specified value of the Multiprotocol Label Switching (MPLS) experimental (EXP) field as a match criterion.
Step 16	Router(config-cmap)# match mpls experimental topmost values	(Optional) Matches the MPLS EXP value in the topmost label.
Step 17	Router(config-cmap)# match not match-criteria	(Optional) Specifies the single match criterion value to use as an unsuccessful match criterion.
Step 18	Router(config-cmap)# match packet length {max maximum-length-value [min minimum-length-value] | min minimum-length-value [max maximum-length-value]}	Optional) Specifies the Layer 3 packet length in the IP header as a match criterion in a class map.
Step 19	Router(config-cmap)# match port-type {routed | switched}	{routed | switched} (Optional) Matches traffic on the basis of the port type for a class map.
Step 20	Router(config-cmap)# match [ip] precedence precedence-value [precedence-value precedence-value precedence-value]	(Optional) Identifies IP precedence values as match criteria.
Step 21	Router(config-cmap)# match protocol protocol-name	(Optional) Configures the match criteria for a class map on the basis of the specified protocol. Note: There is a separate match protocol (NBAR) command used to configure network-based application recognition (NBAR) to match traffic by a protocol type known to NBAR.
Step 22	Router(config-cmap)# match protocol citrix [app application-name-string] [ica-tag ica-tag-value]	(Optional) Configures NBAR to match Citrix traffic
Step 23	Router(config-cmap)# match protocol fasttrack file-transfer "regular-expression"	(Optional) Configures NBAR to match FastTrack peer-to-peer traffic.
Step 24	Router(config-cmap)# match protocol gnutella file-transfer "regular-expression"	(Optional) Configures NBAR to match Gnutella peer-to-peer traffic.
Step 25	Router(config-cmap)# match protocol http [url url-string | host hostname-string | mime MIME-type | c-header-field c-header-field-string | s-header-field s-header-field-string]	(Optional) Configures NBAR to match Hypertext Transfer Protocol (HTTP) traffic by URL, host, Multipurpose Internet Mail Extension (MIME) type, or fields in HTTP packet headers.
Step 26	Router(config-cmap)# match protocol rtp [audio | video | payload-type payload-string]	(Optional) Configures NBAR to match Real-Time Transfer Protocol (RTP) traffic.
Step 27	Router(config-cmap)# match qos-groupqos-group-value	qos-group-value (Optional) Identifies a specific QoS group value as a match criterion.
Step 28	Router(config-cmap)# match source-address mac address-destination	(Optional) Uses the source MAC address as a match criterion.
Step 29	Router(config-cmap)# match start {l2-start | l3-start} offset number size number {eq | neq | gt | lt | range range | regex string} {value [value2] | [string]}	(Optional) Configures the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3).
Step 30	Router(config-cmap)# match tag {tag-name}	(Optional) Specifies tag type as a match criterion.
Step 31	Route(config-cmap)# exit	(Optional) Exits class-map configuration mode.

Creating a traffic policy

To configure a traffic policy (sometimes also referred to as a policy map), use the **policy-map** command. The **policy-map** command allows you to specify the traffic policy name and also allows you to enter policy-map configuration mode (a prerequisite for enabling QoS features such as traffic policing or traffic shaping).

Associate the Traffic Policy with the Traffic Class

After using the **policy-map** command, use the **class** command to associate the traffic class (created in the "Creating a Traffic Class" section) with the traffic policy.

The syntax of the **class** command is as follows:

class *class-name*
no class *class-name*

For the *class-name* argument, use the name of the class you created when you used the **class-map** command to create the traffic class (Step 3 of the "Creating a Traffic Class" section).

After entering the **class** command, you are automatically in policy-map class configuration mode. The policy-map class configuration mode is the mode used for enabling the specific QoS features.

Procedure

To create a traffic policy (or policy map) and enable one or more QoS features, perform the following steps.

	This procedure lists many of the commands you can use to enable one or more QoS features. For example, to enable Class-Based Weighted Fair Queuing (CBWFQ), you would use the bandwidth command. Not all QoS features are available on all platforms or in all Cisco IOS releases. For the features and commands available to you, see the Cisco IOS documentation for your platform and version of Cisco IOS software you are using.

Configuration Steps		
	Command or Action	**Purpose**
Step 1	Router> enable	Enables privileged EXEC mode.
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# policy-map policy-name	Creates or specifies the name of the traffic policy and enters policy-map configuration mode.
Step 4	Router(config-pmap)# class {class-name |class-default}	Specifies the name of a traffic class (previously created in the "Creating a Traffic Class" section) and enters policy-map class configuration mode.
	Use one or more of the following commands to enable the specific QoS feature you want to use.	
Step 5	Router(config-pmap-c)# bandwidth {bandwidth-kbps | percent percent }	(Optional) Specifies a minimum bandwidth guarantee to a traffic class in periods of congestion. A minimum bandwidth guarantee can be specified in kbps or by a percentage of the overall available bandwidth.
Step 6	Router(config-pmap-c)# fair-queue number-of-queues	(Optional) Specifies the number of queues to be reserved for a traffic class.
Step 7	Router (config-pmap-c)# police bps [burst-normal][burst-max] conform-	(Optional) Configures traffic policing.

Configuration Steps		
	Command or Action	**Purpose**
	action action exceed-action action [violate-action action]	
Step 8	Router(config-pmap-c)# priority {bandwidth-kbps | percent percentage} [burst]	(Optional) Gives priority to a class of traffic belonging to a policy map.
Step 9	Router(config-pmap-c)# queue-limit number-of-packets	(Optional) Specifies or modifies the maximum number of packets the queue can hold for a class configured in a policy map.
Step 10	Router(config-pmap-c)# random-detect [dscp-based | prec-based]	(Optional) Enables Weighted Random Early Detection (WRED) or distributed WRED (DWRED).
Step 11	Router(config-pmap-c)# set atm-clp	(Optional) Sets the cell loss priority (CLP) bit when a policy map is configured.
Step 12	Router(config-pmap-c)# set cos {cos-value | from-field [table table-map-name]}	(Optional) Sets the Layer 2 class of service (CoS) value of an outgoing packet.
Step 13	Router(config-pmap-c)# set discard-class value	(Optional) Marks a packet with a discard-class value.
Step 14	Router(config-pmap-c)# set [ip] dscp {dscp-value | from-field [table table-map-name]}	(Optional) Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte.
Step 15	Router(config-pmap-c)# set fr-de	(Optional) Changes the discard eligible (DE) bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface.
Step 16	Router(config-pmap-c)# set precedence {precedence-value | from-field [table table-map-name]}	(Optional) Sets the precedence value in the packet header.
Step 17	Route(config-pmap-c)# set mpls experimental value	(Optional) Designates the value to which the MPLS bits are set if the packets match the specified policy map.
Step 18	Router (config-pmap-c)# set qos-group {group-id | from-field [table table-map-name]}	(Optional) Sets a QoS group identifier (ID) that can be used later to classify packets.
Step 19	Router(config-pmap-c)# service-policy policy-map-name	(Optional) Specifies the name of a traffic policy used as a matching criterion (for nesting traffic policies [hierarchical traffic policies] within one another).
Step 20	Router(config-pmap-c)# shape {average | peak } mean-rate [burst-size [excess-burst-size]]	(Optional) Shapes traffic to the indicated bit rate according to the algorithm specified.
Step 21	Router(config-pmap-c)# exit	(Optional) Exits policy-map class configuration mode.

Attaching a Traffic Policy to an Interface

To attach a traffic policy to an interface, use the **service-policy** command. The **service-policy** command also allows you to specify the direction in which the traffic policy should be applied (either on packets coming into the interface or packets leaving the interface).

The **service-policy** command syntax is as follows:
service-policy {**input** | **output**} *policy-map-name*
no service-policy {**input** | **output**} *policy-map-name*
Procedure

To attach a traffic policy to an interface, perform the following steps.

	Depending on the platform and Cisco IOS release you are using, a traffic policy can be attached to an ATM permanent virtual circuit (PVC) subinterface, a Frame Relay data-link connection identifier (DLCI), or another type of interface.

	Command or Action	Purpose
Step 1	Router> enable	Enables privileged EXEC mode.
Step 2	Router# configure terminal	Enters global configuration mode
Step 3	Router(config)# interface serial0	Configures an interface type and enters interface configuration mode.
Step 4	Router(config-if)# service-policy output [type access-control] {input | output} policy-map-name	Attaches a policy map to an interface.
Step 5	Router (config-if)# exit	(Optional) Exits interface configuration mode.

	Multiple traffic policies on tunnel interfaces and physical interfaces are not supported if the interfaces are associated with each other. For instance, if a traffic policy is attached to a tunnel interface while another traffic policy is attached to a physical interface with which the tunnel interface is associated, only the traffic policy on the tunnel interface works properly.

Verifying the Traffic Class and Traffic Policy Information

To display and verify the information about a traffic class or traffic policy, perform the following steps.

	Command or Action	Purpose
Step 1	Router> enable	Enables privileged EXEC mode.
Step 2	Router# show class-map [type {stack | access-control}] [class-map-name]	(Optional) Displays all class maps and their matching criteria.
Step 3	Router# show policy-map policy-map class class-name	(Optional) Displays the configuration for the specified class of the specified policy map.
Step 4	Router# show policy-map policy-map	(Optional) Displays the configuration of all classes for a specified policy map or all classes for all existing policy maps.
Step 5	Router# show policy-map interface [type access-control] type number [vc [vpi/] vci] [dlci dlci] [input | output]	(Optional) Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface.
Step 6	Router# exit	(Optional) Exits privileged EXEC mode.

Using the CBQoS data

Once Polling has been started, reports can be viewed under the CBQoS tab. Reporting is available in terms of Volume of Traffic, Number of Packets, Traffic Speed and Queue. The pre-policy, post-policy and drops in different traffic class along with the queuing status enables you to validate the efficiency of your QoS settings.Individual graphs are displayed for Pre Policy, Post Policy and Dropped. Pre Policy refers to the state before the CBQoS policy was applied. Post Policy refers to the state after the CQoS policy is applied. Dropped gives information on the packets that are dropped as a result of applying the policies.

Based on these information suitable correction can be done to the policies to make it best suit the business goals of the organization.

User Management

The **User Management** option lets view the different users with varying access privileges that have been created. The users defined in OpManager can access NetFlow Analyzer. Adding, removing and modifying users is possible only from OpManager.

The administrative privileges for each user are described below:

Privilege	Administrator	Operator
View all available devices and IP groups	✓	✗
Create, modify, or delete device groups or IP groups	✓	✗
Modify Runtime Administration properties	✓	✗
Change other users' passwords	✓	✗
Manage licensed interfaces	✓	✗
Apply different licenses	✓	✗
Create other Administrator users	✓	✗
Create other Operator users	✓	✗
Create other Guest users	✓	✓ *
Add, modify, or delete Alerts	✓	✓ **
Enabling and Disabling Alerts	✓	✓ ***
Add, modify, or delete applications	✓	✓
Change device settings	✓	✓
View traffic reports	✓	✓
View custom reports	✓	✓
Assigned to one or more device groups or IP groups	✗	✓
Scheduling of Reports	✓	✗
NBAR Configuration	✓	✗
Viewing NBAR Reports	✓	✓

***** only within the assigned group
****** It is not possible to delete a Link Down Alert
******* Link Down alert can be enabled or disabled only by Administrator

License Management

The **License Management** option lets you manage the interfaces exporting NetFlow data to NetFlow Analyzer, depending on the license that you have purchased. To access the License Management option, from OpManager go to Admin-> License Management.

The status box at the top of the page indicates the type of license currently applied, the total number of interfaces currently managed, and the number of days remaining for the license to expire.

Contact support@opmanager.com for upgrading your license.

The Router List shows all the routers and interfaces from which NetFlow exports are received, and whether they are managed or not.

Applying License for enabling the NetFlow Analyzer plug-in

Click here to apply the license for enabling the NetFlow Analyzer plug-in. The process of applying NetFlow Analyzer plug-in license is the same as the one that is followed for applying OpManager license.

Note: If you have already running NetFlow Analyzer separately in your network, you can use the same license for the plug-in also.

Managing a router/interface

To select the router and all its interfaces check the checkbox next to the router name. To select a specific interface, check the checkbox next to the interface name.

Once you have selected the required interfaces, click the **Manage** button to manage these interfaces. This means that flows received from these interfaces will be processed by NetFlow Analyzer, and traffic graphs and reports can be generated.

The maximum number of interfaces that can be managed, depends on the current license applied.

Unmanaging a router/interface

To select the router and all its interfaces check the checkbox next to the router name. To select a specific interface, check the checkbox next to the interface name.

Click the **Unmanage** button to unmanage these interfaces. This means that flows received from these interfaces will be dropped by NetFlow Analyzer. Once unmanaged, these interfaces will not be seen on the Dashboard or be listed in device groups.

However they will still be listed in the Router List in the License Management page.

Unmanaging an Interface will lead to bill generation for the particular interface, IF that interface has been selected for billing.

Deleting a router/interface

To select the router and all its interfaces check the checkbox next to the router name. To select a specific interface, check the checkbox next to the interface name.

Click the **Delete** button to delete these interfaces. This means that these interfaces are completely removed from all screens of the NetFlow Analyzer client.

However, if flows are still being sent from these interfaces to NetFlow Analyzer, they will reappear in the Dashboard. To prevent this, you need to disable NetFlow export from those interfaces.

Licensing New Interfaces

If a NetFlow packet is received from a new interface, and the number of interfaces presently managed is less than that allowed in the current license, this interface is listed under Router List on the Dashboard with a message saying new flows have been received. You need to then click the **License Management** option and change this interface's status to Managed in order to include this interface in the list of managed interfaces, and also generate traffic graphs and reports for the same.

If a NetFlow packet is received from a new interface, and the number of interfaces presently managed is equal to that allowed in the current license, you need to either unmanage any other managed interfaces, and then manage this interface, or leave this interface in **New** status. In any case graphs and reports can be generated only for managed interfaces.

Sync NetFlow

If a name or IP address of a device that exports flow to NetFlow Analyzer, it continues to export flows to NetFlow Analyzer but the details are not updated in OpManager for that device. However, by default after 15 minutes the device details and data are updated in OpManager. If required you can update the details immediately in OpManager by click Sync NetFlow link (OpManager-> Admin-> Sync NetFlow).

Integrating with Other ME Applications

Integrating with NetFlow Analyzer

OpManager can seamlessly integrate with the network traffic monitoring tool, Netflow Analyzer, one of the AdventNet ManageEngine suite of products. Netflow Analyzer provides detailed interface traffic reports.

To view the detailed traffic report from Netflow Analyzer, the prerequisites are,

1. Netflow Analyzer must be up and running in your network
2. The interface whose traffic you would like to monitor must be discovered in both, OpManager and Netflow Analyzer.
3. The NetFlow Analyzer settings must be configured properly in OpManager

Configure NetFlow Analyzer Settings

To configure the NetFlow Analyzer Settings in OpManager

1. Click **Admin** tab, click **Add-On/Products Settings**
2. Click **NetFlow Settings** icon in this screen
3. Type the following NetFlow Analyzer server details:
    1. Server Name
    2. Port (default is 8080)
    3. User Name
    4. Password
    5. Polling Interval in mins
4. Save the settings.

After configuring the settings, you can follow the steps given below to see the detailed reports:

1. Go to the Routers map
2. Click the required interface icon in the Routers map to see its snapshot page
3. In the Interface Traffic details column, do a mouse-over the **Netflow** icon. Select
    1. Top Applications
    2. Top Sources
    3. Top Destinations
    4. Top Conversations

Traffic details are shown in detail based on the above options.

Integrating with ServiceDesk Plus

If you have ServiceDesk Plus installed in your network, you can automatically log trouble tickets from OpManager for specific network faults. So, besides the provision to email, sms, or notify fault in other forms, you can also track the faults by logging trouble tickets to ServiceDesk Plus. This helps in issue tracking.

For logging the trouble ticket to ServiceDesk Plus correctly, you need to ensure the following:

1. Incoming Mail Settings must be configured properly in ServiceDesk Plus
2. ServiceDesk Plus Settings must be configured in OpManager
3. A notification profile to log a trouble ticket to ServiceDesk Plus must be configured and associated.

Configure Servers Settings

Following are the steps to configure the ServiceDesk Plus and OpManager Server settings:

1. Configure Incoming Mail Settings in ServiceDesk Plus
2. Configure Mail Server Settings in OpManager
3. OpManager must 'know' where ServiceDesk Plus resides to log the ticket. To configure the ServiceDesk Plus settings details, follow the steps given below
4. Click **Admin** tab, and select **Add-On/Products Settings** and configure the following values:

   Server where ServiceDesk Plus is running: Name or the IP address of the machine where ServiceDesk Plus is installed and running.

   ServiceDesk Plus server port number : The port number in which the ServiceDesk Plus application is running. Default port is 8080.

   ServiceDesk Plus login: The user name with which you will log in into ServiceDesk Plus. Default is **admin**

   ServiceDesk Plus password : The password to log in into ServiceDesk Plus. Default password for **admin** user is **admin**

   HelpDesk Email Address : The email address in the mail server to which the email must be sent. This should be the same as configured in the mail-server settings in ServiceDesk Plus. Example: help@servicedeskplus.com

   From Email Address : The initiator's email address. Example: requestor@company.com

After the settings are configured correctly, you can configure a notification profile to log a trouble ticket.

Integrating with DeviceExpert

OpManager can seamlessly integrate with the DeviceExpert, a network change and configuration management solution for network devices. The configurations of devices like routers, switches, and firewalls can be managed using this solution. When integrating with OpManager, you can monitor the devices and their resources for performance, and also manage changes and configurations across these devices.

To view the configuration and the changes from OpManager,

1. DeviceExpert must be up and running in your network
2. The network devices whose changes you want to monitor must be discovered in both, OpManager and DeviceExpert.
3. The DeviceExpert settings must be configured properly in OpManager

Configure DeviceExpert Settings

To configure the DeviceExpert Settings in OpManager

1. Copy the file server.keystore from /DeviceExpert/conf folder to a folder on your local machine.
2. From OpManager WebClient, select **Admin** tab and click on **Add-On/Products Settings**
3. Click **DeviceExpert Settings** link in this screen
4. Type the following DeviceExpert server details:
    1. Server Name
    2. Port (default is 6060)
    3. Browse and select the server.keystore file copied to the local machine.
    4. User Name
    5. Password
    6. Hit **Test Connection and Save** option to verify the integration.

After configuring the settings, you can follow the steps given below to see the detailed reports:

1. Go to the snapshot page of the Router/Switch/Firewall
2. From the **Device Info** menu, select **Startup Configuration** to see the initial configuration of the device.
3. From the same menu, select **Running Configuration** to see the runtime configuration changes made to the device.

Troubleshooting

What to do when you encounter an error message 'Unable to fetch values from DeviceExpert, The server might not be running or the network traffic may be too high' when configuring the DeviceExpert details in OpManager:

- Check if the DeviceExpert service details are correctly configured. Specially, the port number and the proper server.keystore file is selected.
- Despite correct details, if you still face issues, try the following:
    - Open a command prompt and change directory to /opmanager/bin
    - Execute the script ssl_deviceexpert.bat with the absolute path of OpManager installation folder. For instance, if the OpManager path is C:\Program Files\AdventNet\ME\OpManager, the script should be executed as follows:

      C:\Program Files\AdventNet1\ME\OpManager\bin>ssl_deviceexpert.bat "C:\Program Files\AdventNet1\ME\OpManager"

Integrating with Firewall Analyzer

OpManager can seamlessly integrate with Firewall Analyzer, a web-based Firewall Log Analysis & Reporting Tool. Integrating OpManager with Firewall Analyzer allows you to monitor your Server's Security, Traffic, & Bandwidth utilization in depth.

To view the detail traffic and security reports from Firewall Analyzer, the prerequisites are,

1. Firewall Analyzer must be up and running in your network
2. The firewall whose logs you would like to analyze must be available in both, OpManager and Firewall Analyzer. That is, configure your firewalls to forward syslog messages to the server running Firewall Analyzer. These firewalls should be discovered in OpManager for monitoring.
3. The Firewall Analyzer settings must be configured properly in OpManager.

Configure Firewall Analyzer Settings

To configure the Firewall Analyzer Settings in OpManager

1. Click **Admin** tab, click **Add-On/Products Settings**
2. Click **Firewall Analyzer Settings** icon in this screen
3. Type the following Firewall Analyzer server details:
    1. Server Name
    2. Port (default is 8500)
    3. User Name
    4. Password
    5. Select the Polling Interval in minutes
4. Test and save the settings by clicking on **Test Connection and Save** button.

After configuring the settings, you can follow the steps given below to see the detailed reports:

1. Go to the Firewalls map
2. Click the required Firewall icon in this map to see its snapshot page
3. From the **Reports** menu on the right in the snapshot page, select any of the following options to view the respective reports:
    1. Traffic Reports
    2. Security Reports
    3. Custom Reports
    4. All Reports

Detailed reports retrieved from Firewall Analyzer are shown based on the reports selected.

Other Utilities and Tools

Configuring Database Maintenance

To plot graphs and generate reports, OpManager collects data from the managed devices at regular intervals. By default, OpManager aggregates the performance data into hourly data at the end of each hour. The hourly data thus calculated will be aggregated into daily data at the end of each day. These aggregated data will be used in graphs and reports.

OpManager allows you to maintain the database with the required data. By default, the detailed data will be maintained for 7 days, the hourly data for 30 days and the daily data for 365 days. After the specified period, the database will be cleaned up automatically.

To configure your own settings for database maintenance, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Tools**, click **Database Maintenance**.
3. Specify the values for the following fields:
    1. **Alarms Database**- the maximum number of recent alarms to be maintained must be specified here. For instance, if you want an history of last 500 alarms, specify the value as 500 here.
    2. **Events Database**- multiple events correlate to generate a single alarm. This is essentially a history information.
    3. **Performance Database**- the cleanup interval of the raw data as well as the archived data must be specified here.
4. Click **OK** to apply the changes.

Scheduling Downtime

Maintenance of network devices forms an integral part of network administration. You may want to perform a maintenance of specific device types at specific intervals. If such devices are removed from the network, or rebooted, then you will see alarms indicating that the device, or the applications in the device are unavailable. Since the devices are not available when polled for status during the maintenance period, unnecessary alarms are fired. To prevent the devices from being monitored for status during maintenance, you can schedule a maintenance task for such devices.

Following are the steps:

1. From the **Admin** tab, select **Downtime Scheduler** option under **Tools**.
2. Click on **New Schedule**.
3. In the **New Downtime Schedule** form, provide the following details:
    - Schedule Name
    - Schedule Description
    - Select the Status as **Enabled**, if you want the Scheduled task to take effect immediately. Else select **Disabled**, so that you can enable it when required.
    - Select the frequency at which the Task has to be scheduled/executed. It can be **Once**, **Every Day**, **Every Week**.
    - Specify the start and end time/day of the task in the corresponding fields.
    - If it is a schedule to be executed **every day**, then specify the date from which the task must be scheduled.
    - You can assign the task to only the required devices, or a device category like switches, routers, to a Business view, or to URL Monitors.

The schedule will be executed as configured.

Scheduling Reports

OpManager allows you schedule a new report and also to schedule a generated report.

Schedule a new report

1. From Admin tab, select **Select Schedule Reports** under **Tools**.
2. In the Report Scheduler page, click the **Add Schedule** button on the right.
3. Configure the following details:

    1. **Name**: Configure a name for the schedule.
    2. **Choose Report Type**: You can choose to schedule reports for specific devices, top n devices, or for all devices.
    3. Click **Next**.

Scheduling Top N Reports / All Devices reports:

If you have selected to schedule the Top N Reports, configure the following details:

1. **Top N Reports**: Select from Top 10/25/50/100 reports.
2. **Period**: Choose the period for which you want the report scheduled.
3. **Select Report(s)**: Select the required resource reports to be scheduled.
4. **Business View Reports**: Select the relevant check-box and the business view to generate reports specific to the devices in that business view.
5. Click **Next**.

Scheduling Device specific Availability reports:

f you have chosen to schedule reports for device specific availability details, configure the following:

1. Select either a category of devices, or the required business view, or select specific devices manually for generating the availability reports.
2. Select the period for which you want to generate the reports.
3. Click **Next**.

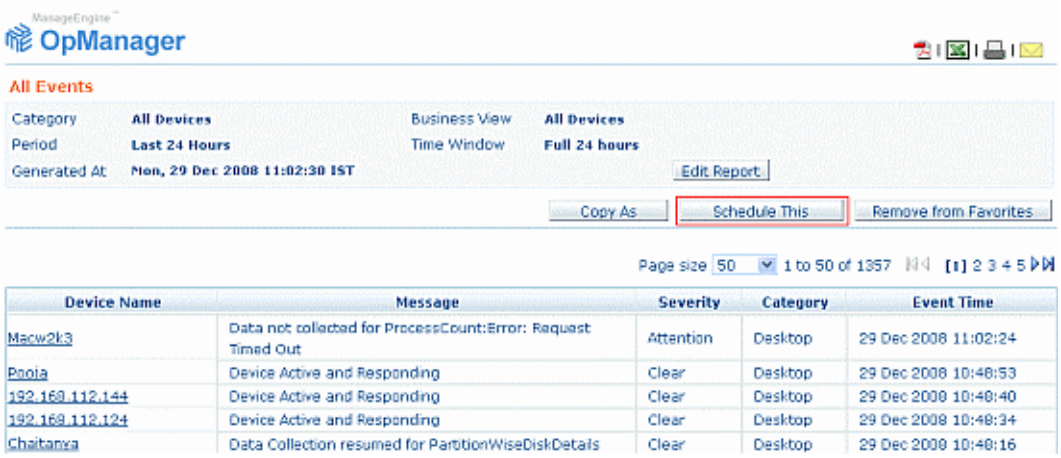
Configuring the Time Settings for generating reports:

1. **Daily**: Select the time at which the reports must be generated every day.
2. **Weekly**: Select the time and also the days on which the reports must be generated.
3. **Monthly**: Select the time, day, and the months for which the reports must be generated.
4. **Report Format Type**: Select either PDF or XLS to receive the report in the respective formats.
5. **Report Delivery**: Select any one of the following options.
    - Configure the email ids to which the reports are to be sent as attachments. [or]
    - Configure the url where the reports can be published.
6. **Period**: Choose the period for which you want the report scheduled.
7. **Select Report(s)**: Select the required resource reports to be scheduled.
8. Click **Next**.

Verify the details of the configured schedule and hit **Submit** for the schedule to take effect.

Scheduling a generated report

1. In the report page that is generated, click **Schedule This** button to schedule the report.



2. Enter the report name.
3. Select the time and period.
4. Enter the email ID to which the report has to be delivered.
5. Click **OK**.

Enabling the Configured Schedule

Once you configure the report schedules, they are listed in the Report Schedule page (Admin --> Schedule Reports page). Select the required schedules and click on the **Enable** button at the bottom of the list. You can also disable or delete a schedule from here.

Using the Quick Configuration Wizard

OpManager's quick configuration wizard helps you to configure monitors, notification profiles, dependency, and so on, for many devices at a time.

To invoke the wizard, in the **Admin** tab under **Configuration**, click **Quick Configuration wizard**. You can perform the following configurations for multiple devices:

- Assign a notification profile to several devices
- Delete associated notification profile
- Add a new service monitor to several devices
- Add a windows service monitor to several devices.
- Associate Event log rules to several devices
- Configure Device Dependencies
- Associate a credential to several devices
- Delete devices
- Manage / Unmanage devices

MIB Browser: Overview

The MIB Browser tool is a complete SNMP MIB Browser that enables loading and browsing MIBs and allows you to perform all SNMP-related operations. You can also view and operate on the data available through the SNMP agent running on a managed device.

The features of MIB Browser include the following:

- Saving the MIB Browser settings.
- Loading and viewing MIB modules in a MIB tree.
- Traversing the MIB tree to view the definitions of each node for a particular object defined in the MIB.
- Performing the basic SNMP operations, such as GET, GETNEXT, GETBULK, and SET.
- Support for multi-varbind requests. This feature is available only in the Java client.
- Real-time plotting of SNMP data in a graph. Line graph and bar graph are the two types of graphs that are currently supported. This feature is available only in the Java client.
- Table-view of SNMP data. This feature is available only in the Java client.
- Enables loading of MIBs at startup. This feature is available only in the Java client.

MIB Browser Interface

- **Menu bar**: Contains menus with related commands to perform all administrative operations.
- **Toolbar**: Contains frequently used administrative commands for easy access.
- **MIB Tree**: Shows all the loaded MIBs. You can traverse the tree and view the definition of each node in the tree.
- **SNMP Settings**: Displays the SNMP settings of the selected node.
- **Result Display Area**: Displays the result of the SNMP operations.
- **Object Attributes**: Shows the attributes of the selected node

Switch Port Mapper

OpManager shows the connectivity between a switch and other connected devices in the network in Switch Port Mapper. You get the details such as the MAC address, IP Address and DNS names of the devices connected to the switch.

You need to provide the details such as the community string and port number of the switch and if needed, the details of the server or router that may contain the layer 3 details.

To view the switch port mapping details, follow the steps given below:

1. Click the switch icon in the map.
2. In the displayed Snapshot page, click **Switch Port Mapper** under **Device Info**.
3. Click **Show Mapping** in the Switch Port Mapper window to view the mapping details.

Reporting

About Reports

Intuitive dashboards and detailed reports helps you determine the performance of your network in very less time. OpManager allows you to export the default reports to other file formats such as exporting to PDF or XLS. You can also schedule the reports to be emailed or published. The default reports available in OpManager include:

- **System**: Provides a complete report on all the system related activities of all the devices. This category of reports include All Events, All Down Events, SNMP Trap Log, Windows Event Log, Performance Monitor Log, Notification Profiles Triggered, Downtime Scheduler Log, Schedule Reports Log, All Alerts and All Down Alerts.
- **Health and Performance**: Gives you a detailed report on the health and performance of all/top N devices.
- **Availability and Response**: Gives you a detailed report on the availability and the response time of all/top N devices
- **Inventory**: Inventory reports are available for servers, desktops, all devices, SNMP-enabled devices and non-SNMP devices.
- **WAN Monitors**: Gives you a detailed report on RTT threshold violation, RTT trend, link availability and error statistics and Top N paths with Maximum threshold violation and RTT. (Also can be accessed from Maps-> WAN Monitors-> Reports)
- **VoIP Monitors**: Gives you a detailed report on the Jitter, MOS, RTT etc. history and top N call paths by Jitter, MOS, Packet loss and Latency. (Also can be accessed from Maps-> VoIP Monitors-> Reports)
- **My Favorites**: OpManager provides the option to categorize all your important and frequently viewed reports as you favorites.

Note: Exporting WAN Monitor and VoIP Monitor reports to XLS format is not supported at present.

Viewing Device Health Report at a Glance

Performance of various resources on a device can impact the health of that device. For instance, it can be due to insufficient hardware, high resource utilization of a resource by a process, too many processes running on that system, or too much incoming and out-going traffic, or even network latency.

OpManager helps you see the performance of all the resources at a glance for a single device. This helps troubleshooting the problem much easier.

To access this report, go to the device snapshot page and click on **At a Glance Report** option on the right corner. This is a report showing the device health at a glance. It shows details like the availability, response time, packet loss, resource utilizations etc.

Viewing Interface Reports

Interface reports help you to determine the health of the interface by generating detailed reports on In and Out Traffic, In and Out Errors and Discards, Bandwidth & Outage Report, At-a-Glance Report etc. The reports can be exported to PDF format, taken printouts or emailed by clicking the respective icons. To generate the interface reports, follow the steps given below:

1. Go to the snapshot page of the interface whose health report you want to generate.
2. Click on **Reports** tab available on the top right of the page. All the default reports that can be generated are listed.
3. Click on the name of the required report to generate current day's report. Click on the 7 or 30 days icon to generate the report for the last 7 or 30 days respectively.

Business View-based Reports

OpManager provides an intuitive Availability Dashboard for your business view. You can track the fault to the root in no time.

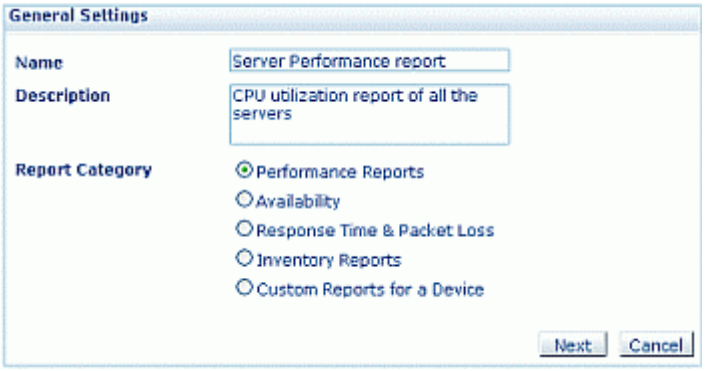
To access the business view dashboard, follow the steps below:

1. Go to the required business view.
2. Click on the **Dashboard** tab. The business view dashboard shows the availability distribution and also the least available devices in that view.
3. Click on the bar indicating a problem to drill down to the actual fault.
4. You can also view the dashboard for various periods like the last 24 hours, or last few days to analyze the trend.

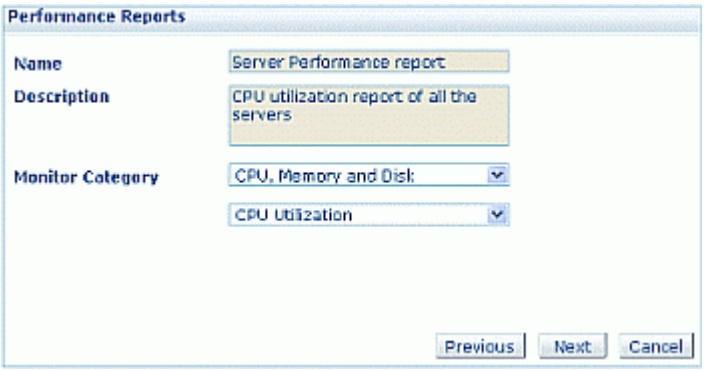
Creating New Reports

Custom Reports option is replaced with Create New Reports option. The big advantage with Create New Reports option is that you can create your own reports, save them and generate whenever required. To create a new report follow the steps given below:

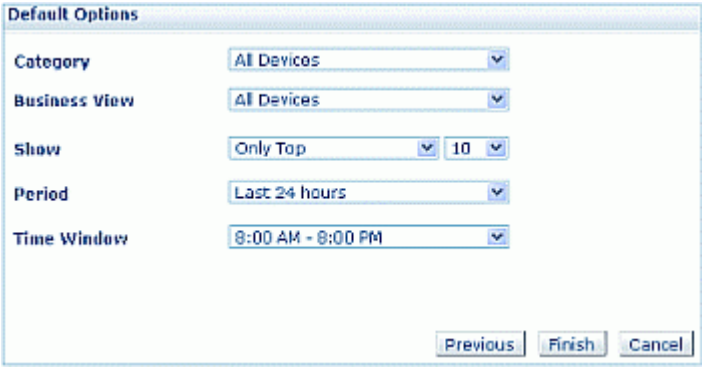
1. Click the **Create New Report** button under the Reports tab. Create New Report window opens.



2. Enter a unique **Name** and brief **Description**.
3. Select the required **Report Category**. For instance, the report category is selected as Performance Reports.
4. Click **Next**.



5. Select the **Monitor category**.
6. Select the sub category.
7. Click **Next**.



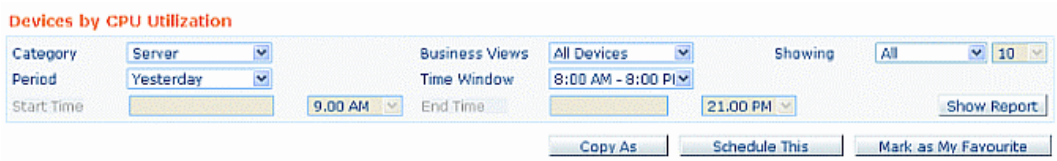
8. Select the required **Category**, **Business Views**, **Top N devices**, **Period** and **Time Window**.
9. Click **Finish** to create the new report.

The created report gets saved under the appropriate report category. Go to that category and click on the report to generate the report.

Editing Reports

OpManager allows you to edit a generated report in order to refine for some specific parameters, devices or time periods. To edit a generated report follow the steps given below:

1. Click **Edit** report button available on the top right of the report page.
2. Change the required fields. The various fields that can be altered are Category, Period, Business Views, Time Window and Top N devices.

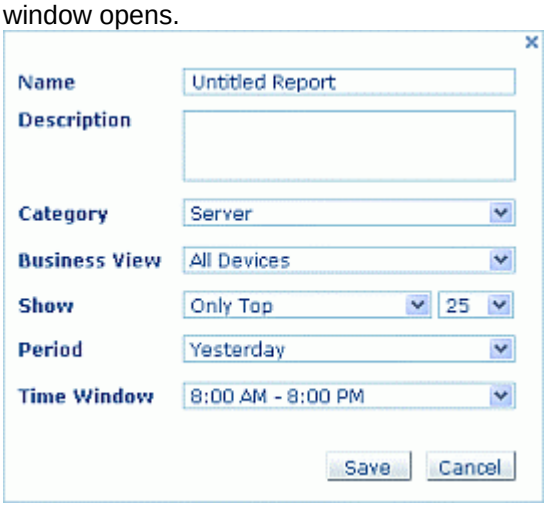


3. After modifying the required fields, click on **Show Report** to generate the report effecting the changes made.

Copying Reports

OpManager allows you to copy a generated report in order to retain the already configured parameters as template and do some minor changes on them and save as a new report. To copy and save a report follow the steps given below:

1. Click **Copy As** button available on the top middle of the report that is generated. A small window opens.



2. Enter a unique **Name** and a brief **Description**.
3. Change the required fields. The various fields that can be altered are Category, Period, Business Views, Time Window and Top N devices.
4. After modifying the required fields, click **Save** button to save the new report.

Configuring Favorite Reports

With OpManager you can mark the reports that are frequently viewed as Favorite reports. The reports that are marked as favorite reports are listed under My Favorites report category. To mark a report as your favorite one, follow the steps given below:

1. Generate the report that you want to mark as your favorite.
2. Click **Mark as My Favorite** button available on the top right of the report.

A message is displayed saying that "This report has been marked as your favorite".

Deleting a report from the Reports

To delete a report from your favorites list, follow the steps given below:

1. Go to **Reports**-> **My Favorites**.
2. Click the respective delete icon ✖ of the report that you want to remove from your favorites list. A confirmation dialog box opens.
3. Click **OK** to confirm deleting.

Note: Default reports available under My Favorites category cannot be deleted.

[or]

1. Generate the report that you want to remove from your favorites list.
2. Click **Remove from Favorites** button available on the top right of the report.

A message is displayed saying that " This report has been removed from your favorites list".

Time Based Availability Reports

You can generate time based availability reports of the devices from Reports-> Default reports-> Detailed reports. In the report page that is generated select the desired time name form the Time Window box available under **Report Options** in order to generate the report for that particular time period alone. You can add/modify/delete a time name from the Time Window box.

To add/modify/delete a time name open the Report Config file (\OpManager\Conf) with Notepad/word pad.

Add Time Name:

Enter a new time window name as given below in the Report Config file.

```
<Root>
   <Configurations>
      <TimeWindow Name="Full 24 hours" Value="0-24"/>
      <TimeWindow Name="8:00 AM - 8:00 PM" Value="8-20" />
      <TimeWindow Name="6:00 AM - 9:00 PM" Value="6-21" /> [New Time Window Name. Enter your desired values.]
   </Configurations>
</Root>
```

Modify Time Name:

Modify the existing time window name as given below in the Report Config file.

```
<Root>
   <Configurations>
      <TimeWindow Name="Full 24 hours" Value="0-24"/>
      <TimeWindow Name="10:00 AM - 10:00 PM" Value="10-22" /> [Existing Time Window Name that is modified. Enter your desired values.]
   </Configurations>
</Root>
```

Delete Time Name:

To delete an existing time window name simply delete that time window name in the Report Config file.

Note: After adding/modifying/deleting a time name restart the OpManager.

Appendix

Installing SNMP Agent on Windows System

(Adapted from Windows help)

- Installing SNMP Agent on Windows XP/2000/2003
- Installing SNMP Agent on Windows NT
- Installing SNMP Agent on Windows 98

You need to know the following information before you install the Simple Network Management Protocol (SNMP) service on your computer:

- Community names in your network.
- Trap destinations for each community.
- IP addresses and computer names for SNMP management hosts.

To install SNMP on Windows XP, 2000, and 2003, follow the steps given below:

You must be logged on as an administrator or a member of the Administrators group to complete this procedure. If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.

- Click **Start**, point to **Settings**, click **Control Panel**, double-click **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
- In Components, click **Management and Monitoring Tools** (but do not select or clear its check box), and then click **Details**.
- Select the **Simple Network Management Protocol** check box, and click **OK**.
- Click **Next**.
- Insert the respective CD or specify the complete path of the location at which the files stored.
- SNMP starts automatically after installation.

This completes the installation process. This also implements the Host Resources MIB automatically. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

To install SNMP in Windows NT, follow the steps given below:

- Right-click the **Network Neighborhood** icon on the Desktop.
- Click **Properties**.
- Click **Services**.
- Click **Add**. The Select Network Service dialog box appears.
- In the Network Service list, click **SNMP Service**, and then click **OK**.
- Insert the respective CD or specify the complete path of the location at which the files stored and click **Continue**.
- After the necessary files are copied to your computer, the Microsoft SNMP Properties dialog box appears.

This completes the installation process. This also implements the Host Resources MIB automatically. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

To install SNMP in Windows 98

Make sure your Windows 98 CD is in the drive. Then follow the steps given below:

- On the **Network** control panel, click **Add**.
- Double-click **Service** in the Select Network Component Type dialog box.
- Click **Have Disk** in the Select Network Service dialog box.
- Type the path to the "TOOLS\RESKIT\NETADMIN\SNMP" directory on your computer's CD drive in the Install From Disk dialog box and then click **OK**.
- Select **Microsoft SNMP agent** from the **Models** list in the Select Network Service dialog box and then click **OK**.

This completes the installation process. This also implements the Host Resources MIB automatically. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

Installing SNMP on Linux Systems

The installation of new version of SNMP is required only for versions prior to 8.

Download the latest rpm version of SNMP using the following URL:

http://prdownloads.sourceforge.net/net-snmp/net-snmp-5.1.1-1.rh9.i686.rpm?download

Download the zip version of SNMP using the following URL:

http://heanet.dl.sourceforge.net/sourceforge/net-snmp/ucd-snmp-4.2.6.tar.gz

To **install using the rpm**, follow the steps given below:

1. Login as "root" user.
2. Before installing the new version of net-snmp, you need to remove the earlier versions of net-snmp in your machine. To list the versions of net-snmp installed in your machine, execute the following command:

   rpm -qa | grep "net-snmp"
3. If there are already installed version in your machine, remove them using the command:

   rpm -e <version of net-snmp listed as the output for previous command> --nodeps
4. If there are no previously installed versions in your machine, then execute the following command to install the new version:

   rpm -i <new downloaded version of SNMP agent> --nodeps

To **install using the zip**, follow the steps given below:

Extract the file using following command:

tar -zxvf ucd-snmp-4.2.6.tar.gz

To install SNMP, follow the steps given below:

1. Login as *root* user.
2. Execute the command to set the path of the C compiler:
   export PATH=<gcc path>:$PATH
3. Execute the following four commands from the directory where you have extracted the ucd-snmp:
   - *./configure --prefix=<**directory_name**> --with-mib-modules="host"*

     directory_name is the directory to install SNMP agent. Preferably choose a directory under /root. The directories /usr and /local might contain the files of an older version of SNMP and so do not choose these directories to ensure proper installation.
   - make
   - umask 022
   - make install

This completes the installation process. For configuring SNMP agents to respond to SNMP requests, refer to Configuring SNMP agents.

Installing SNMP Agent on Solaris Systems

Download the latest version of SNMP using the following URL:

http://heanet.dl.sourceforge.net/sourceforge/net-snmp/ucd-snmp-4.2.6.tar.gz

Extract the file using following command:

tar -zxvf ucd-snmp-4.2.6.tar.gz

To install SNMP, follow the steps given below:

1. Login as *root* user.
2. Execute the command to set the path of the C compiler:
   export PATH=<gcc path>:$PATH
3. Execute the following four commands from the directory where you have extracted the ucd-snmp:
   - *./configure --prefix=<**directory_name**> --with-mib-modules="host"*

     directory_name is the directory to install SNMP agent. Preferably choose a directory under /root. The directories /usr and /local might contain the files of an older version of SNMP and so do not choose these directories to ensure proper installation.
   - make
   - umask 022
   - make install

This completes the installation process. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

Configuring SNMP Agents

Configuring SNMP Agent in Windows XP, 2000, and 2003 Systems

For details about installing SNMP agents in Windows systems, refer to Installing SNMP Agent on Windows Systems.

To configure SNMP agent in Windows XP and 2000 systems, follow the steps given below:

1. Click **Start**, point to **Settings**, click **Control Panel**.
2. Under Administrative Tools, click **Services**.
3. In the details pane, right-click **SNMP Service** and select **Properties**.
4. In the **Security** tab, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.
5. Under Accepted community names, click **Add**.
6. Under **Community Rights**, select a permission level for this host to process SNMP requests from the selected community.
7. In **Community Name**, type a case-sensitive community name, and then click **Add**.
8. Specify whether or not to accept SNMP packets from a host:
    - To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.
    - To limit acceptance of SNMP packets, click **Accept SNMP packets from these hosts**, click **Add**, type the appropriate host name, IP or IPX address, and then click **Add** again.
9. Click **Apply** to apply the changes.

To configure SNMP traps, follow the steps given below:

1. Click **Start**, point to **Settings**, click **Control Panel**.
2. Under Administrative Tools, click **Services**.
3. In the details pane, right-click **SNMP Service** and select **Properties**.
4. In the **Traps** tab, under **Community name**, type the case-sensitive community name to which this computer will send trap messages, and then click **Add** to list.
5. Under **Trap destinations**, click Add.
6. In the **Host name, IP or IPX address** field, type host name or its IP address of the server (OpManager server) to send the trap, and click **Add**.
7. Repeat steps 5 through 7 until you have added all the communities and trap destinations you want.
8. Click **OK** to apply the changes.

Configuring SNMP Agent in Windows NT Systems

For details about installing SNMP agents in Windows systems, refer to Installing SNMP Agent on Windows Systems.

To configure SNMP agent in Windows NT systems, follow the steps given below:

- Click **Start**, point to **Settings**, click **Control Panel**.
- Under Administrative Tools, click **Services**.
- In the details pane, right-click **SNMP Service** and select **Properties**.

- In the **Security** tab, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.
- Under **Accepted Community Names**, click **Add**.
- In the **Community Names** box, type the community name to authenticate the SNMP requests.
- To move the name to the **Accepted Community Names** list, click **Add**.
- Repeat steps 6 and 7 for any additional community name.
- To specify whether to accept SNMP packets from any host or from only specified hosts, click one of two options:
    - **Accept SNMP Packets From Any Host**, if no SNMP packets are to be rejected on the basis of source computer ID.
    - **Only Accept SNMP Packets From These Hosts**, if SNMP packets are to be accepted only from the computers listed. To designate specific hosts, click Add, type the names or addresses of the hosts from which you will accept requests in the IP Host or IPX Address box, and then click Add.
- Repeat step 11 for any additional hosts.
- In the **Agent** tab, specify the appropriate information (such as comments about the user, location, and services).
- Click **OK** to apply the changes.

Further, the SNMP Agent running Windows NT does not respond to Host Resource Data, by default. To include this support, you should have Windows NT Service Pack 6 & above. Verify this and then follow the steps given below:

- Extract the NTHR-MIB.zip available at http://bonitas.adventnet.com/opmanager/09Sep2004/NTHR-MIB.zip into C:\WinNT\system32 folder.
- Double click on the registry files to import the mibs into Windows registry.
- Restart your Windows NT box.

To Configure SNMP Traps, follow the steps given below:

- Click **Start**, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Services**.
- In the details pane, click **SNMP Service**, and then click **Properties**.
- Click the **Traps** tab.
- To identify each community to which you want this computer to send traps, type the name in the **Community Name** box. Community names are case sensitive.
- After typing each name, click **Add** to add the name to the list.
- To specify hosts for each community you send traps to, after you have added the community and while it is still highlighted, click **Add** under Trap Destination.
- To move the name or address to the Trap Destination list for the selected community, type the host name in the **IP Host/Address or IPX Address** box, and then click **Add**.
- Repeat step 10 for any additional hosts.
- Click **OK** to apply the changes.

Configuring the Agent in Linux versions prior to 8

For details about installing SNMP agents in Linux systems, refer to Installing SNMP Agent on Linux Systems.

- Stop the agent if it is running already using the command:
  /etc/rc.d/init.d/snmpd stop
- Make the following changes in **/etc/rc.d/init.d/snmpd** file
  - Replace the line
    daemon /usr/sbin/snmpd $OPTIONS
    with
    daemon /root/ucd_agent/sbin/snmpd $OPTIONS
  - Replace the line
    killproc /usr/sbin/snmpd
    with
    killproc /root/ucd_agent/sbin/snmpd

    This is to choose the current installed version while starting and stopping the SNMP agent.
- Start the agent using the command */etc/rc.d/init.d/snmpd start*.

Configuring the Agent in Linux versions 8 and above

On Linux versions 8 and above, the latest version of SNMP will already be available. You need to just make the following changes in **snmpd.conf** file:

- Insert the line
  view allview included .1.3.6
  next to the line
  # name incl/excl subtree mask(optional)
- Change the line
  access notConfigGroup "" any noauth exact systemview none none
  next to the line
  # group context sec.model sec.level prefix read write notif
  as
  access notConfigGroup "" any noauth exact allview none none
- Then restart the snmp agent using the following command:

  /etc/rc.d/init.d/snmpd restart

Configuring the Agent in Solaris Systems

For details about installing SNMP agents in Solaris systems, refer to Installing SNMP Agent on Solaris Systems.

- Stop the agent if it is running already using the following command:

  /etc/init.d/init.snmpdx stop

- Make the following changes in **/etc/init.d/init.snmpdx** file

  - Replace the lines

    if [-f /etc/snmp/conf/snmpdx.rsrc -a -x /usr/lib/snmp/snmpdx]; then
    /usr/lib/snmp/snmpdx -y -c /etc/snmp/conf -d 3 -f 0
    fi

    with

<Installation Directory>/sbin/snmpd

- Replace the line

  /usr/bin/pkill -9 -x -u 0 '(snmpdx|snmpv2d|mibiisa)'

  with

  /usr/bin/pkill -9 -x -u 0 '(snmpd)'

- Restart the agent using the following command:

  /etc/init.d/init.snmpdx start.

Configuring SNMP Agent in Cisco Devices

For configuring SNMP agents in Cisco devices, you need to log into the device and switch to privileged mode.

Use the following set of commands listed below to enable SNMP:

To enable SNMP:

From the command prompt, run the following commands:

#configure terminal
#snmp-server community <community_string> rw/ro (example: snmp-server community public ro)
#end
#copy running-config startup-config

To enable trap:

Again, from the command prompt, run the following commands:

#configure terminal
#snmp-server enable traps snmp authentication
#end
#copy running-config startup-config

To set OpManager as host:

Run the following commands from the command prompt:

#configure terminal
#snmp-server host <OpManager server running system's IP> <Trap community string> snmp (example: snmp-server host 192.168.9.58 public snmp)
#end
#copy running-config startup-config

Configuring SNMP Agent in Lotus Domino Server

The Domino SNMP Agent is configured as a Windows Service and is set up to run automatically. This means that once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino you should stop the LNSNMP and Windows SNMP Services before beginning the upgrade process.

- Stop the LNSNMP and SNMP services. Enter these commands:

  net stop lnsnmp
  net stop snmp

- Configure the Lotus Domino SNMP Agent as a service. Enter this command:

  lnsnmp -Sc

- Start the SNMP and LNSNMP services. Enter these commands:

  net start snmp
  net start lnsnmp

Configuring SNMP Agent in MSSQL Server

Verify whether SNMP agent is running in the server. If the agent is not installed in the server, refer to Installing SNMP Agent on Windows System and Configuring SNMP agents for installing and configuring SNMP agent.

Then, start the SQLSERVERAGENT service following the steps given below:

In **Windows 2000/XP**:

- Click **Start**, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Computer Management**.
- In the console tree, click **Services and Applications** and then click **Services**.
- Right-click **SQLSERVERAGENT** and click **Start.**

In **Windows NT**:

- Right-click on the **Network Neighborhood** icon on the Desktop.
- Click **Properties**.
- Click **Services**.
- Right-click **SQLSERVERAGENT** and click **Start**.

Configuring SNMP Agent in Oracle Server

To collect data from the Oracle servers and to receive traps from them using OpManager, you need to install and configure Oracle Intelligent Agent. The Oracle Intelligent Agent supports SNMP, allowing third-party systems management frameworks to use SNMP to receive SNMP traps directly from the Agent. By configuring the Agent to recognize SNMP requests from the master agent, third-party systems can gather relevant data.

In Windows machines

1. Once you have installed and configured the SNMP agents in your Windows machines, you have to integrate SNMP with Intelligent agent. This requires Oracle Peer SNMP Master Agent and SNMP Encapsulator Agent to be installed in the Oracle server. Note that these agents must be the same version as the Intelligent Agent and installed in the same ORACLE_HOME.

After the installation completes, the following new NT services will be created: Oracle SNMP Peer Encapsulator Oracle Peer SNMP Master Agent.

If you do not install the Intelligent Agent software in the default $ORACLE_HOME, the names of all the services will begin with the following: Oracle<home name>

For SNMP master agent to communicate with both the standard SNMP service and the Intelligent Agent, the SNMP services file must be configured properly.

Specify an unused port where the encapsulated agent, Microsoft SNMP Service, should be listening. Microsoft SNMP Service typically uses port 1161. The port is specified in the SERVICES file located in the NT_HOME\SYSTEM32\DRIVERS\ETC directory.

Make sure that you have the following lines in the file:
snmp 1161/udp snmp
snmp-trap 1162/udp snmp
Note: If an entry for SNMP already exists in the file, change the port from 161 (default number) to another available port (1161 in this example).

2. In the same location, check that the HOSTS and LMHOSTS.SAM files contain the mappings of IP addresses to host names for all computers in the SNMP setup. System performance will improve if more computer addresses can be resolved locally. Even if you use DHCP and WINS, adding the IP addresses will speed up the SNMP integration.