

## **Administrator Guide**

<http://www.adventnet.com>  
nms-support@adventnet.com

**AdventNet, Inc.**  
5200 Franklin Dr, Suite 115  
Pleasanton, CA 94588 USA

**Phone:** +1-925-924-9500  
**Fax:** +1-925-924-9600  
**Email:** [info@adventnet.com](mailto:info@adventnet.com)

## Table Of Contents

<b>6.1 ABOUT THIS DOCUMENT.....</b>	<b>6</b>
<b>6.2 DATABASE CONFIGURATION .....</b>	<b>8</b>
6.2.1 Configuring Database for Web NMS .....	9
6.2.2 Using Oracle Replication in Web NMS .....	15
6.2.3 Using MySQL Replication in Web NMS.....	24
<b>6.3 DISCOVERING YOUR NETWORK .....</b>	<b>30</b>
6.3.1 Using Discovery Configurator .....	31
6.3.1.1 Opening Discovery Configurator.....	32
6.3.1.2 General Configuration.....	33
6.3.1.3 Protocol Configuration .....	39
6.3.1.4 Network Specific Discovery .....	43
6.3.1.5 Device Specific Discovery .....	47
6.3.1.6 Criteria Based Discovery .....	52
6.3.2 Device and Network Discovery Options .....	55
6.3.3 Configuring Discovery Filters.....	58
6.3.4 ManagedObject UI Settings.....	59
6.3.5 Setting User Privileges .....	61
6.3.6 Configurable Discovery Parameters.....	63
<b>6.4 CONFIGURING MAPS .....</b>	<b>64</b>
6.4.1 Map UI Settings .....	65
6.4.2 Setting User Privileges .....	67
<b>6.5 FAULT MANAGEMENT .....</b>	<b>69</b>
6.5.1 Configuring Trap Ports.....	70
6.5.2 Configuring Trap Parsers.....	71
6.5.3 Configuring Event Parsers.....	77
6.5.4 Configuring Event Filters .....	83
6.5.5 Configuring Alarm Filters .....	92
6.5.6 Performing Alarm Operations .....	98
6.5.7 Setting User Privileges .....	100
6.5.8 Configurable Parameters.....	102

<b>6.6 CONFIGURATION MANAGEMENT .....</b>	<b>103</b>
6.6.1 Configuring Tasks.....	104
6.6.2 Reusable Tasks .....	110
6.6.3 Creating Device Lists.....	116
6.6.4 Executing Tasks .....	118
6.6.5 Executing Default Tasks .....	123
6.6.6 Auditing.....	132
6.6.7 Configurable Parameters.....	136
<b>6.7 PERFORMANCE MANAGEMENT .....</b>	<b>137</b>
6.7.1 Performance Management: Getting Started .....	138
6.7.2 Configuring Data Collection .....	139
6.7.2.1 Selecting Devices for Data Collection .....	142
6.7.2.2 Defining the Data to be Collected .....	145
6.7.2.3 Managing Data Collection Configuration .....	148
6.7.3 Adding Statistics at Runtime.....	149
6.7.4 Defining Thresholds.....	155
6.7.4.1 Using User Interface .....	158
6.7.4.2 Using Configuration File .....	160
6.7.4.3 Associating Threshold with Statistics.....	162
6.7.5 Clearing the Data.....	163
6.7.6 Setting User Privileges .....	164
6.7.7 Configurable Parameters.....	165
<b>6.8 SECURITY MANAGEMENT .....</b>	<b>166</b>
6.8.1 Managing Groups .....	167
6.8.1.1 Adding Groups .....	168
6.8.1.2 Assigning Users to Groups .....	169
6.8.1.3 Deleting Users from Groups .....	170
6.8.1.4 Configuring Authorized Scopes .....	171
6.8.1.5 Managing Custom View Scopes.....	173
6.8.1.6 Deleting Groups .....	177
6.8.2 Managing Users.....	178
6.8.2.1 Adding Users .....	179
6.8.2.2 Changing User Profile.....	182
6.8.2.3 Assigning Groups to Users .....	184
6.8.2.4 Changing User Password .....	185

6.8.2.5 Managing Audit Trails .....	186
6.8.2.6 Deleting Users .....	189
6.8.3 Managing Operations .....	190
6.8.3.1 Understanding Default Operations .....	191
6.8.3.2 Assigning Operations.....	197
6.8.3.3 Adding Operations .....	199
6.8.3.4 Deleting Operations .....	200
6.8.4 Authorization for Security Operations .....	201
6.8.5 Security Management - Configurable Parameters.....	204
6.8.6 Security Management: An Example .....	205
<b>6.9 PROVISIONING .....</b>	<b>207</b>
6.9.1 Invoking Provisioning Templates .....	208
6.9.2 Scheduling and Provisioning Templates.....	210
6.9.3 Deleting and Reloading Templates.....	211
6.9.4 Working with ActivityList .....	212
6.9.5 Setting User Privileges .....	214
<b>6.10 POLICY MANAGEMENT .....</b>	<b>216</b>
6.10.1 Configuring Policies .....	217
6.10.2 Accessing Policies .....	220
6.10.3 Viewing Default Policy Details .....	224
<b>6.11 ADMINISTRATION TOOLS .....</b>	<b>235</b>
6.11.1 Runtime Administration.....	236
6.11.2 SNMPv3 Security Configuration .....	238
6.11.3 Status Viewer.....	239
<b>6.12 GENERAL ADMINISTRATION .....</b>	<b>241</b>
6.12.1 Configuring Log Settings .....	242
6.12.2 Creating Custom Views .....	245
6.12.3 Working with Telnet and SSH Session to a Device .....	246
<b>6.13 ADVANCED ADMINISTRATIVE TASKS .....</b>	<b>254</b>
6.13.1 Front End Server Administration.....	255
6.13.2 Configuring Transport Mechanism.....	259
<b>6.14 ADMINISTRATION THROUGH WEB CLIENT .....</b>	<b>261</b>
6.14.1 Admin Configurations .....	262
6.14.2 Admin Operations .....	267
6.14.3 Server Details .....	269

6.14.4 Module Details .....	272
6.14.5 Web Client: User Administration.....	274
6.14.6 Web Client: Network Administration .....	276
<b>6.15 SIMULATORS AND BROWSERS.....</b>	<b>279</b>
6.15.1 MIB Browser .....	280
6.15.1.1 Starting Up .....	281
6.15.1.2 Configuration.....	283
6.15.1.3 MIB Operations .....	288
6.151.3.1 Loading MIBs .....	289
6.151.3.2 Unloading MIBs.....	293
6.151.3.3 Parsing MIBs.....	294
6.151.4 SNMP Operations.....	296
6.15.1.4.1 SNMP GET .....	297
6.15.1.4.2 SNMP GETNEXT.....	299
6.15.1.4.3 SNMP GETBULK.....	300
6.15.1.4.4 SNMP SET.....	301
6.15.1.5 Trap Handling .....	303
6.15.1.5.1 Viewing Traps .....	304
6.15.1.5.2 Parsing Traps.....	307
6.15.1.5.3 Creating Parser Files .....	310
6.15.1.5.4 Editing Parser Files.....	312
6.15.1.6 Table Handling.....	313
6.15.1.6.1 Retrieving Table Data .....	314
6.15.1.6.2 Adding Rows .....	317
6.15.1.6.3 Deleting Rows .....	319
6.15.1.7 Graphs .....	320
6.15.1.7.1 Line Graph .....	321
6.15.1.7.2 Bar Graph.....	324
6.15.1.8 Internationalization.....	326
6.15.1.9 Debugging and Decoding .....	328
6.151.10 Error Messages.....	331
6.15.1.11 Customization .....	336
6.15.1.12 FAQs.....	338
6.15.2 TL1 Craft Interface .....	340
6.15.2.1 Getting Started.....	341

6.15.2.2 Working with TL1 Craft Interface .....	346
6.15.2.2.1 How to Establish a Connection with the TL1 Device? .....	347
6.15.2.2.2 How to Manage Multiple Connections? .....	351
6.15.2.2.3 How to Send and Receive Messages?.....	352
6.15.2.2.4 How to Send and Receive Bulk Messages?.....	354
6.15.2.2.5 How to View Log Messages?.....	355
6.15.2.3 Files Used by TL1 Craft Interface.....	357
6.15.2.4 How to Configure TL1 Craft Interface? .....	358
6.15.2.5 Internationalization.....	361
6.15.2.6 Re-branding TL1 Craft Interface.....	363
6.15.3 CLI Browser: An Introduction.....	364
6.15.3.1 Overview .....	366
6.15.3.2 Connecting Devices.....	370
6.15.3.3 Loading Files.....	374
6.15.3.4 Configuring Message Parameters .....	375
6.15.3.5 Sending CLI Command .....	378
6.15.3.6 Executing Scripts .....	380
6.15.3.7 Terminal Transformation.....	381
6.15.3.8 Enabling Special Characters .....	382
6.15.3.9 Debugging Message .....	383
6.15.3.10 Command Generation .....	385
6.15.3.11 Internationalization.....	389
<b>APPENDIX .....</b>	<b>390</b>
Appendix A: Discovery.....	391
Appendix B: Fault .....	399
Appendix C: Performance.....	407

## 6.1 About This Document

As network administrators / system engineers are primarily responsible for managing enterprise and service provider infrastructure, this **Administrator Guide** helps you configuring Web NMS to suit your organizational requirements and facilitates integrating new management services. The administrative tasks are eased by Web NMS by providing easy-to-use graphical user interfaces which enables you to perform all administrative tasks quickly.

The administrative tasks that you can perform using a Web Client are explained in a separate chapter Administration through Web Client. Hence all other chapters explain the administrative tasks that can be performed using the Application, Applet, or Web Start Clients.

### Contents

- Configuring Database
- Discovering Your Network
- Configuring Maps
- Fault Management
- Configuration Management
- Performance Management
- Security Management
- Provisioning
- Policy Management
- Administration Tools
- General Administration
- Advanced Administrative Tasks
- Administration through Web Client
- Simulators and Browsers
- Appendix

### Document Conventions

To understand the conventions used across the Administrator Guide, click Help  provided on the top frame of the Administrator Guide.

### Product Support

- For technical support, send an e-mail to [nms-support@adventnet.com](mailto:nms-support@adventnet.com).
- For contact information, refer to Contact page on our Web site [www.adventnet.com](http://www.adventnet.com).

### Related Documents

- For information on installing the product, refer to Installation Guide.
- For information on using the Web NMS Clients and performing user tasks, refer to User Guide.
- For information on Web NMS product features, refer to Quick Tour.
- For complete list of Web NMS documents, refer to Product Documentation page on our Web site.

## Viewing Help

### To view Web NMS Help

From **Help** menu, choose **Help Contents**. An HTML file with links to all Web NMS documents is displayed in a Web browser (the default browser that has been configured in your system).

### To view context-sensitive help in Application Client, do any of the following

Context-sensitive help displays appropriate Help topic which assists you to get specific information about whatever part of the client you are using at any given moment.

- Press **F1** on any dialog box or window (or)
- Click the **Help** button on the toolbar in a window.

A help file associated with the screen you are working on is displayed.

### To view context-sensitive help in Application Client dialog boxes

Click the **Help** button.

## 6.2 Database Configuration

This chapter helps you in configuring Web NMS to support various databases. It also explains how you can setup database replication.

---

- Configuring Database for Web NMS
  - Using Oracle Replication in Web NMS
  - Using MySQL Replication in Web NMS
-

## 6.2.1 Configuring Database for Web NMS

This topic explains the steps to be followed to configure various databases with Web NMS.

Most of the RDBMS, which are JDBC compliant and use a JDBC driver, are supported by Web NMS. The databases that are tested extensively and supported are listed below:

Most of the RDBMS, which use a JDBC driver are supported by Web NMS. The databases that are tested and supported are:

- MySQL
- Oracle
- MSSQL
- Sybase
- Solid
- TimesTen
- Firebird

---

For information on the supported database versions and the corresponding database drivers, refer to Software Requirements in Installation Guide.

### Configuring Web NMS for MySQL

MySQL is the default database bundled with Web NMS. Hence configuration is not required. For information on supporting MySQL 4.x, refer to To run Web NMS with MySQL 4.x section.

Web NMS starts and initializes this database before starting the Web NMS modules. In Windows and Solaris, the MySQL daemon is started when **startnms** script file located in the <Web NMS Home>/bin directory is invoked. In Linux, you need to start the MySQL daemon as a service before starting the Web NMS Server. To start MySQL daemon as a server in Linux, perform the following steps.

1. Log in as a super user.
2. Start MySQL. **Syntax:** \$ /etc/rc.d/init.d/mysql start

If you have modified any of the default settings and later if you need to configure for MySQL database, perform the following procedure.

1. If the Web NMS Server is already started, then do a proper shutdown of server. Do not terminate the process abnormally or abruptly.
2. Run **reinitialize\_nms** script file located in the <Web NMS Home>/bin directory to clean up the tables in the database.
3. Copy the **database\_params.conf** and the **DatabaseSchema.conf** file located in the <Web NMS Home>/conf/MySQL directory to the <Web NMS Home>/conf directory.
4. In **database\_params.conf** file, specify the machine name where the database is to run, user name, and password for the database.
5. Edit the **setEnv** script file located in <Web NMS Home> directory and set the **DB\_CLASSPATH** variable as <Web NMS Home>/mysql/mmm.mysqlDriver/mysql\_comp.jar. <Web NMS Home> is where you have installed Web NMS.
6. Start the MySQL Server, by running the **startMySQL** script file located in the <Web NMS Home>/bin directory.
7. Start Web NMS Server.

## Supporting MySQL 4.x

By default, Web NMS runs with MySQL 3.23.58 which is bundled with the product. To run Web NMS with MySQL 4.x, perform the following procedure.

### To run Web NMS with MySQL 4.x

1. Copy the file **snmpDatabaseSchema.config** located in <Web NMS Home>/conf/MySQL directory to <Web NMS Home>/conf directory.
2. Edit this file **snmpDatabaseSchema.config** and change the column name **LOCALTIME** in **USMTABLE** to some other value, e.g., **USMLOCALTIME**.

**Example:**

# ColumnKey	ColumnName	Datatype
# LOCALTIME	<b>USMLOCALTIME</b>	VARCHAR(30)

**Note:** Change only the ColumnName and retain the ColumnKey and Datatype.

3. Edit the file **DatabaseSchema.conf** located in <Web NMS Home>/conf directory and change the column name **LOCALTIME** in **USMTABLE** to the same value as configured in **snmpDatabaseSchema.config**.

**Example:** USMLOCALTIME varchar(30)

This change is done, because MySQL 4.x has LOCALTIME as a reserved keyword.

4. To create MySQL tables as **InnoDB** tables, start the **mysql daemon** with the following option.

```
--default-table-type=InnoDB
```

[**Note:** The above line is case sensitive]

For information on specifying this option, refer to  
[http://dev.mysql.com/doc/mysql/en/Program\\_Options.html](http://dev.mysql.com/doc/mysql/en/Program_Options.html)

5. Edit the **setEnv** script file located in <Web NMS Home>. By default, the MySQL home is set as

```
set MYSQL_HOME=%NMS_HOME%\mysql
```

Change the MySQL home to the directory where you have installed MySQL 4.x.

## Configuring MySQL Home

It is not mandatory to keep the MySQL directory (having the full MySQL installation) under <Web NMS Home>. The path for the MySQL files is configurable and hence the MySQL directory can be present anywhere.

### To set the MySQL home

1. Edit the **setEnv** script file located in <Web NMS Home> directory.
2. Set the **MYSQL\_HOME** variable to the location (full directory path) where MySQL is installed.

### To set the MySQL home (while using Launcher)

If you use the Web NMS Launcher for starting Web NMS, and if you want to configure the MySQL home perform the following configuration.

In **launcher\_conf.txt** file located in the <Web NMS Home>/conf file, for reinitializing the database, specify the MySQL home as:

```
<application>
<property name="AppName" value="Reinitialize Web NMS" />
.....
<property value="-Dmysql.home=./mysql" name="AppJavaOption"/>
</application>
```

In the same file, for starting the Web NMS server, specify the MySQL home as:

```
<application>
<property name="AppName" value="Start Web NMS Server" />
.....
<property name="AppJavaOption" value="-Dmysql.home=./mysql -Dwebserver.port=9090 -D" />
.....
</application>
```

**Note:** When remote connections to a MySQL server running on **Linux 8.0 or Linux 9.0** platforms are attempted, a segmentation fault (*java.sql.SQLException*) is caused and the server gets restarted by **safe\_mysqld**. On the remote side, the client reports a 'Lost connection during query'.

To solve this problem, the parameter "**--skip-name-resolve**" needs to be added in the MySQL startup and MySQL should be restarted.

In **"/usr/bin/safe\_mysqld"** file, add the parameter as follows:



```
...
$NOHUP_NICENESS $!edir/$MYSQLD $defaults -Sg --basedir=$MY_BASEDIR_VERSION
--datadir=$DATADIR $USER_OPTION --pid-file=$pid_file --skip-locking --skip-name-
resolve >> $err_log 2>&1

else

eval "$NOHUP_NICENESS $!edir/$MYSQLD $defaults -Sg --
basedir=$MY_BASEDIR_VERSION --datadir=$DATADIR $USER_OPTION --pid-
file=$pid_file --skip-locking --skip-name-resolve $args >> $err_log 2>&1"
```

### Configuring Web NMS for Oracle

1. If the Web NMS Server is already started, do a proper and normal shutdown of Oracle. Do not terminate the process abruptly.
2. Run **reinitialize\_nms** script file located in the <Web NMS Home>/bin directory to clean up the tables in the database.
3. Edit the **setEnv** script file located in the <Web NMS Home> directory. Set the **DB\_CLASSPATH** variable (which is by default set to mysqldriver) to JDBC driver for Oracle.

#### Example:

```
DB_CLASSPATH=<PATH>/classes12.zip
```

<PATH> is the location where **classes12.zip** is located.

3. In Oracle, edit the file **init<database\_name>.ora** located in the <Oracle Home>/Database directory. By default, the number of open cursors supported for a single connection is set as 50. Change it to **250**.
 

```
OPEN_CURSORS 250.
```
4. Start the **TnsListener Service** and then the Oracle database. The TnsListener Service listens for and accepts incoming connection requests from client applications.
5. Copy **DatabaseSchema.conf** and **database\_params.conf** files located in the <Web NMS Home>/conf/Oracle directory to <Web NMS Home>/conf directory.
6. Edit the **database\_params.conf** file and specify the machine name where the database is to run, user name, and password for the database.
7. Ensure that Oracle server is listening to the port **1521**.
8. Start the Web NMS server.

## Configuring Web NMS for MSSQL

1. If the Web NMS Server is already started, do a proper and normal shutdown of Oracle. Do not terminate the process abruptly.
2. Run **reinitialize\_nms** script file located in the <Web NMS Home>/bin directory to clean up the tables in the database.
3. Copy **database\_params.conf** and **DatabaseSchema.conf** files located in the <Web NMS Home>/conf/Mssql directory to <Web NMS Home>/conf directory.
4. Edit the **database\_params.conf** file and specify the machine name where the database is to run, user name, and password for the database.
5. Edit the **setEnv** script file located in the <Web NMS Home> directory. Set the DB\_CLASSPATH with the location of **JTurbo.jar**, which is the JDBC driver for MSSQL.
6. Start the MSSQL Server.
7. Start the Web NMS Server.

## Configuring Web NMS for Sybase ASE 12.5 and Sybase ASA 8.0.2

1. If the Web NMS Server is already started, do a proper and normal shutdown of Oracle. Do not terminate the process abruptly.
2. Run **reinitialize\_nms** script file located in the <Web NMS Home>/bin directory to clean up the tables in the database.
3. Edit the **setEnv** script file located in the <Web NMS Home> directory and set the DB\_CLASSPATH with the location of the JDBC driver for Sybase.

**Example:**

```
set DB_CLASSPATH=<Web NMS Home>/conf/Sybase/jconn2.jar
```

4. Ensure that the **jconn.jar** is placed in the appropriate location as specified in the **setEnv** script file.
5. Copy **DatabaseSchema.conf** and **database\_params.conf** files from the <Web NMS Home>/conf/Sybase directory to the <Web NMS Home>/conf directory.
6. Edit the **database\_params.conf** file and specify the machine name where the database is to run, user name, and password for the database.
7. Ensure if the Sybase server is listening to the port **2048** (for Sybase ASE 12.5) or port **2638** (for Sybase ASA 8.0.2).
8. Start the Web NMS server.

## Configuring Web NMS for Solid

1. If the Web NMS Server is already started, do a proper and normal shutdown of Oracle. Do not terminate the process abruptly.
2. Run **reinitialize\_nms** script file located in the <Web NMS Home>/bin directory to clean up the tables in the database.
3. Edit **setEnv** script file located in the <Web NMS Home> directory and set the DB\_CLASSPATH with the location of the JDBC driver for Solid.

**Example:**

```
set DB_CLASSPATH=%NMS_HOME%conf/Solid/SolidDriver2.0.jar
```

4. Ensure that the jar or zip file containing the required solid jdbc classes is placed in the appropriate location as specified in the **setEnv** script file.
5. Copy **DatabaseSchema.conf** and **database\_params.conf** files from the <Web NMS Home>/conf/Sybase directory to the <Web NMS Home>/conf directory.
6. Edit the **database\_params.conf** file and specify the driver name for Solid database, machine name where the database is to run, user name, and password for the database.
7. Ensure that the Solid server is listening to the port **1313**.
8. Start the Web NMS server.

## Configuring Web NMS for TimesTen

1. If the Web NMS Server is already started, do a proper and normal shutdown of Oracle. Do not terminate the process abruptly.
2. Run **reinitialize\_nms** script file located in the <Web NMS Home>/bin directory to clean up the tables in the database.
3. Edit **setEnv** script file located in the <Web NMS Home> directory and set the DB\_CLASSPATH with the location of the JDBC driver for TimesTen.

**Example:**

```
set DB_CLASSPATH=%NMS_HOME%conf/TimesTen/classes13.jar
```

4. Ensure that the TimesTen driver is placed in the appropriate location as specified in the **setEnv.bat** file.
5. Copy the **DatabaseSchema.conf** file and the **database\_params.conf** file from <Web NMS Home>/conf/TimesTen directory to <Web NMS Home>/conf directory.
6. Edit the **database\_params.conf** file and specify the driver name for TimesTen database, machine name where the database is to run, user name, and password for the database.
7. Ensure if the TimesTen server is listening to the port **14302**.
8. Start the Web NMS server.

## Configuring Web NMS for Firebird

1. Install the Firebird database in your local machine. For information on Firebird version support, refer to Software Requirements.
2. Take a backup of **DatabaseAliases.conf** file located in <Web NMS Home>/conf directory. This backup file can be used later if you want to run Web NMS with any other database other than that of Firebird.
3. Copy the files **snmpDatabaseSchema.config**, **database\_params.conf**, **DatabaseAliases.conf**, and **DatabaseSchema.conf** from the <Web NMS Home>/conf/Firebird/ directory to the <Web NMS Home>/conf directory.

4. Edit the **database\_params.conf** file located in the <Web NMS Home>/conf directory and specify the JDBC URL.

**For Linux:**

Suppose, if you have created the **WebNmsDB** under /opt/interbase/bin directory, then specify the JDBC URL as:

```
jdbc:firebirdsql:/opt/interbase/bin/WebNmsDB (localhost)
jdbc:firebirdsql:nms-clienttest1/3050:/opt/interbase/bin/WebNmsDB
(remotehost)
```

where, **nms-clienttest1** refers to the remote host in which Firebird runs.

**For Windows:**

If you have created the **WebNmsDB** under c:\john\1.0.3\FireBird\bin, then give the JDBC URL as:

```
jdbc:firebirdsql:nms-
clienttest1/3050:c:/john/1.0.3/FireBird/bin/WebNmsDB
```

5. Unzip Firebird driver file. Edit the **setEnv** script file located in <Web NMS Home> and include the **firebirdsql-full.jar** and **firebirdsql.jar** from the zip in **DB\_CLASSPATH**.

**Example:**

```
DB_CLASSPATH=:/home/<machine_name>/driver/firebirdsql-
full.jar:/home/rajagopal/driver/firebirdsql.jar
```

6. Start the Web NMS server.

**To create WebNmsDB in Firebird**

1. Execute **isql.exe** located in *Firebird\bin* directory, where Firebird is installed.
2. A command prompt is displayed with the following message.

```
Use CONNECT or CREATE DATABASE to specify a database
SQL>
```

3. In the SQL prompt, execute the following command to create **WebNmsDB**:

```
SQL>create database 'WebNmsDB' user 'sysdba' password
'masterkey';
```

This creates **WebNmsDB** under *Firebird\bin* directory.



**Note:** Firebird support is not provided for development using Web NMS Studio.

## 6.2.2 Using Oracle Replication in Web NMS

---

- [How Does Database Replication Work](#)
- [Procedure to Setup Database Replication](#)
  - [Installing Oracle](#)
  - [Creating Databases](#)
  - [Creating / Setting Up Oracle Net8 Names](#)
  - [Creating Users](#)
  - [Creating Tables](#)
  - [Replication Setup](#)
  - [Setting Up Master Site and Master Definition Site](#)
  - [Creating Database Links for Replication](#)
  - [Creating Master Groups at the Master Definition Site](#)
  - [Generating Replication Support](#)
  - [Starting Replication Activity](#)
  - [Configurations to be done in Web NMS](#)
  - [Starting Web NMS with Database Replication](#)

---

The design of Web NMS is such that both Primary and Standby servers share the same database. In this scenario, if the database crashes (most unlikely) both the BE and the FE would lose their connection and eventually go down. Though Web NMS does not provide out-of-the-box support for database failover, users can use various mechanisms offered by Oracle such as Oracle Replication and Oracle Clustering for handling database failure.

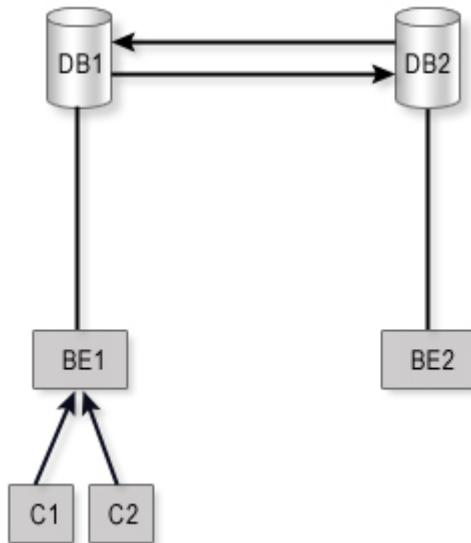
This topic explains how database replication works and the procedure to set up the database to support replication.

### How Does Database Replication Work?

Assume that you have

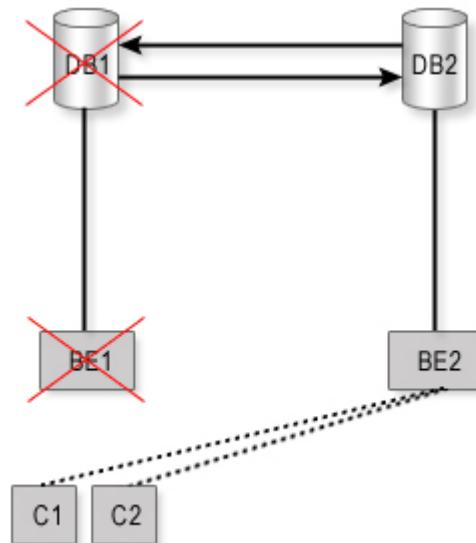
- Web NMS Primary (**BE1**) running in Machine 1 with Database **DB1**.
- Web NMS Standby (**BE2**) in Machine 2 with database **DB2**.
- Clients **C1** and **C2** connected to BE1.
- Set up database replication, so that the database takes care of replicating the contents of DB1 to DB2 continuously. Hence DB1 and DB2 are in synchronization with each other at any point.

This scenario is depicted in the following image.



### What happens when DB1 fails?

In the above given scenario, when the database **DB1** that is connected to **BE1** fails,



- The Primary Server BE1 connected to that also goes down (fails).
- BE2 takes over the functions of BE1. Web NMS automatically takes care of BE failover.
- BE2 continues to use DB2 (replicated database).
- Clients C1 and C2 that were connected to BE1, will switch their connection to BE2.

### What happens when BE1 fails?

In the above scenario, when the primary server **BE1** fails,

- BE2 connected to DB2 will take over the functions of BE1 automatically.
- Clients C1 and C2 that were connected to BE1, will switch their connection to BE2.

## What happens when connection between BE1 and DB1 fails?

If DB1 and BE1 are in different machines and the network connection between them fails,

- BE2 connected to DB2 will take over the functions of BE1 automatically.
- Clients C1 and C2 that were connected to BE1, will switch their connection to BE2.

As the contents of DB2 are in synchronization with DB1, chances of data inconsistency are ruled out in both the above cases.

## Procedure to Set Up Database Replication

The procedure is explained based on an example with the following names.

- Primary Server - BE1
- Secondary Server - BE2
- Primary Database - DB1
- Secondary Database - DB2

This procedure assumes that the primary database is created in the machine where primary server is installed and secondary database is created in the machine where secondary server is installed. **You can create databases in different machines also, i.e., the primary database need not necessarily be created in primary server machine.**

### Note:

- The procedure explained is based on Oracle Database Replication in Solaris.
- The primary server BE1 should be connected to primary database DB1. Similarly, the secondary server BE2 should be connected to secondary database DB2. For information on setting up this, refer to [Web NMS Configuration](#).
- Both the primary and the secondary servers should have the same license files.
- Dynamic table replication is not supported.

## Installing Oracle

1. Install **Oracle Enterprise Edition** in two machines, BE1 and BE2, where the replication has to be set up. The installation process is similar to normal installation except that replication options have to be enabled during the process.

**Note:** The Oracle database installed should be **Oracle Enterprise Edition** as **Oracle Standard Edition** does not support Advanced Replication Options.

2. Install the Oracle Enterprise Manager to invoke the GUI Oracle Replication Manager for setting up and administering the replication environment.

**Note:** During standard installation all the above are installed by default except for custom installations of Oracle.

## Creating Databases

Create two databases, namely DB1 (primary database) and DB2 (secondary database) in BE1 (primary server) and BE2 (secondary server) respectively. The SID of the database should be unique, i.e., DB1 and DB2.

For information on creating the database, refer to Oracle technical manuals.

After creating the database,

1. Edit the file **init.ora** located in the <Oracle Home>/admin/DB1/pfile directory and make the following changes :

```
GLOBAL_NAMES = TRUE
JOB_QUEUE_PROCESSES = 10
OPEN_CURSORS = 500
```

**Note:** If the parameters are not present, add them. Otherwise, modify the parameters with the above values.

2. Restart the database server.
3. Ensure that the database server and the TNS listener are running.

Follow the same procedure for the database DB2 in the secondary server BE2.

### **Creating / Setting Up Oracle Net8 Names**

Follow this procedure in both the machines - BE1 (where DB1 database is created) and BE2 (where DB2 database is created). This procedure is done to create/setup Oracle Net8 Names to enable the communication between the two databases DB1 and DB2.

1. Login as user oracle
2. Invoke the **Net Configuration Assistant** UI from the shell to set the names:  
shell >> netca  
The wizard will be displayed.
3. Select **Local Net Service Name Configuration** and click **Next**.
4. Select **Add** and click **Next**.
5. Select **Oracle8i database or service** and click **Next**.
6. Enter the database name in the **Service Name** field. This value will be DB2 to connect to the DB2 database from DB1 database. Click **Next**.
7. Select **TCP** and click **Next**.
8. Enter the host name in the **Host Name** field. The host name in this case will be the host where the database DB2 is created. Retain the same port number (1521). Click **Next**.
9. Select **Yes, Perform a test** and click **Next**.
10. On successfully creating the name, appropriate message will be displayed. Click **Change Login**.
11. Change the **user name** as *system* and **password** as *manager*. Click **OK**. Click **Next**.
12. Enter the net service name as <host name of the machine having DB2>. Click **Next**.
13. A message **Would you like to configure another net service name?** will be displayed. Click **No**.
14. Click **Next** in the subsequent screens and click **Finish** in the final screen of the wizard.

Follow the same procedure to create Net8 Service Name for the machine BE2 with database DB2 by giving BE1's SID and host name. For example, net service names can be db2 in the BE1 to connect to DB2 and db1 in BE2 to connect to DB1.

## Creating Users

Create a user where all the application tables (i.e., Web NMS tables) are created, in both the machines - BE1 (where DB1 database is created) and BE2 (where DB2 database is created).

**Note:** The user names created on both the databases should be the same.

For information on creating users, refer to Oracle technical manuals.

## Creating Tables

To set up replication, you should have all the tables created in the user's schema. The tables are to be created only on the Master Definition Site i.e. DB1 (primary database) on BE1 (primary server).

**Tip:** To create the tables, start Web NMS Server. Initially the tables are created and then the processes are started. You can view this in the command prompt. Before the process could start, kill the server. On performing this, the tables are created. Check the Database Schema for data types that Oracle Replication does not support.

**Note:** Oracle supports Number, Date, Varchar, Char, BLOBS, CLOBs data types but does not support the replication of columns that use the LONG datatype.

## Replication Setup

In the machine where primary database (DB1) is created,

1. Login as user **Oracle**
2. Invoke the **Oracle Enterprise Manager Console** UI. From the shell prompt, type **oemapp console**.  
shell >> **oemapp console**.

The **Oracle Enterprise Manager Login** dialog is displayed.

3. Select **Launch standalone** and click **OK**. The Oracle Enterprise Manager (OEM) Console is displayed.
4. The databases will be added by default in the OEM console. If not, manually add the respective databases for which setting up/administering of replication have to be done. Select **Navigator > Add Database To Tree**. The **Add Database To Tree** dialog is displayed.
5. Select the radio button 'Add selected databases from your local tnsnames.ora file ....'. Check on the radio buttons displaying the databases DB1 and DB2 .
6. Click **OK** to add the database to the left side of the tree.

Repeat the same procedure to add the database (DB2) in the same machine BE1 with the host name and SID as DB2.

## Setting Up Master Site and Master Definition Site

1. Login as user Oracle
2. Invoke the **Oracle Enterprise Manager Console** UI. From the shell prompt, type **oemapp console**. The **Oracle Enterprise Manager Login** dialog is displayed.
3. Select **Launch standalone** and click **OK**. The **Oracle Enterprise Manager (OEM) Console** is displayed.

4. On the left-side tree, click **DB1** - the database which is going to act as Master Definition Site.
5. Log in with the user name **system** and password **manager**. Click **OK**.
6. On the tree, traverse to **Distributed > Advanced Replication > MultiMaster Replication**.
7. On the right hand side window pane, click on the link **Setup Master Sites**.
8. Click **Add**. The **Add Site** dialog is displayed. Select the Global site name from the drop-down box. DB1 and DB2 both will be available in that drop-down list, if you had already created it as per the example.
9. Enter password as **manager**. Click **OK**.
10. Click **Next**. Information on Replication Administrator, Propagator, and Receiver Accounts will be displayed. No change is needed in this dialog.
11. A default replication administrator user will be created with user name **REPADMIN** and password **REPADMIN**. Click **Next**.
12. In the **Create Schemas to Organize Replication Objects** dialog, click **Add** to add new schemas to the list.
13. In the **Create Schema** dialog that appears, enter the name of a schema that you want to use to contain replication objects, as well as the password for the schema. In the above case, the schema should be the one created earlier.
14. Click **OK** to add the schema to the list of schemas in the setup wizard. Click **Next**.
15. For the **Scheduled Links**, retain the default purge settings itself that is displayed in the remaining screens.
16. In the final screen, click **Finish** to set up the Master Site.

## Creating Database Links for Replication

**Assumption:** Here the database link is named as solaris1 and solaris2 because these are the host names that the DB1 and DB2 resides. Any names can be given.

### In the DB1 database

```
shell >> sqlplus /nolog
```

```
SQL > connect system/manager
connected
```

```
SQL > create public database link solaris2 using 'db2';
database link created.
```

```
SQL > connect repadmin/repadmin
connected
```

```
SQL > create database link solaris2 connect to repadmin identified by repadmin;
Database link created.
```

### In the DB2 database

```
shell >> sqlplus /nolog
```

```
SQL > connect system/manager
connected
```

```
SQL > create public database link solaris1 using 'db1';
```

database link created.

SQL > connect repadmin/repadmin  
connected

SQL > create database link solaris1 connect to repadmin identified by repadmin;  
Database link created.

**Note:** db2 is the Net Service Name that you have created earlier to point to the DB2 database.

## Creating Master Groups at the Master Definition Site

1. In the left-side tree of the OEM Console window, click DB1 - the database which is going to act as the Master Definition Site.
2. Login as the replication administrator (REPADMIN/REPADMIN)
3. Traverse to **Distributed > Advanced Replication > MultiMaster Replication > Master Group** node of the tree. Right-click and select **Create**. The **Create Master Group** dialog will be displayed.
4. Type a name for the group in **Name** field, say MG1.
5. Select the Object tab and click **Add**.
6. Select the schema (that you have already created) from the drop-down box.
7. Select the **Tables** option in this screen. The objects are displayed in the **Available Objects** field. Select the objects you want to replicate one by one by clicking **Add**.
8. Click **OK**.
9. For an object that does not have the primary key, the **Set Alternate Key** column is displayed. Click **OK** for each screen of the **Set Alternate Key** column. Objects to be replicated are listed.
10. Click the **Master Site** tab to view the master definition site name (DB1).
11. Click **Add** to invoke the **Add master site to the group** dialog.
12. Click **Public database link**. The database link names are listed.
13. Select the database link name in **Available Links** and click **OK**. The **Add Destination to Group** dialog is displayed. Destination name is the name of Master site (DB2).

Note : Here the database links that you created as solaris2 will be displayed.

14. Click **Asynchronous**. Select both the check boxes : **Use existing object** and **Copy row data**.
15. Click **OK To All**. The database name and link are added.
16. Click **Create**.
17. The Master Group should be created without any error. A message Objects created successfully is displayed. Now, the master group **MG1** is created under **DB1 > Distributed > Advanced Replication > MultiMaster Replication > Master Group**.
18. Click **DB1 > Replication > Administration** and click the **Topology** tab. The connection between both the databases DB1 and DB2 can be viewed pictorially.
19. Click the **Schedule** tab to configure the frequency of replication.

## Generating Replication Support

**Note:** Before starting the replication activity, ensure that the replication support is generated for the objects.

1. On the left-side tree, click DB1 - the database which is going to act as Master Definition Site.
2. Go to **Distributed > Advanced Replication > MultiMaster Replication > Master Group > MG1**
3. On the right side pane, click the **Objects** tab. The *status* column should show VALID and the *generation status* column should show GENERATED. This will take time for the replication to be generated for objects.

To make sure that the replication generation is not hung (i.e. generation status column showing 'DOING GENERATION')

4. Click on the DB2 database on the left side tree and connect as repadmin/repadmin.
5. Go to **Distributed > Advanced Replication > Administration**.
6. On the right hand pane, click on the **DBMS jobs** tab.
7. A list of jobs will be displayed. Select the last job and run it manually by clicking the **run** button.
4. Then come back to DB1. Go to **Distributed > Advanced Replication > MultiMaster Replication > Master Group > MG1**
5. Click the **Objects** tab on the right hand pane and see that the replication support is generated for each table and generation status column is showing 'GENERATED' values.

## Starting Replication Activity

1. On the DB1 tree, traverse to **Distributed > Advanced Replication > Multimaster Replication > Master Group > MG1**.
2. In the **General** tab, click **Submit Start Request** to start the replication activity only after replication support for all the objects are generated.

## Configurations to be done in Web NMS

Perform the steps to setup Oracle database in both **primary server (BE1)** and **secondary server (BE2)** by referring to Procedure to Configure AdventNet Web NMS for Oracle section.

In secondary server (BE2), edit the file **FailOver.xml** located in <*Web NMS Home*>/conf directory.

- o Uncomment the <STANDBY> tag.
- o Comment out the PRIMARY HEART\_BEAT\_INTERVAL parameter.
- o Edit the values in <STANDBY> tag based on your requirement.

### Example:

```

<FAILOVER>
  <STANDBY
    FAIL_OVER_INTERVAL="60"
    RETRY_COUNT="1">
    <BACKUP
      ENABLED="TRUE"
      BACKUP_INTERVAL="600" />
  </STANDBY>
</FAILOVER>

```

## **Starting Web NMS with Database Replication**

1. Start the Web NMS primary server BE1.
2. After 2 to 3 minutes, start the Web NMS secondary server BE2.

Now the data present in the primary database DB1 is replicated to the secondary database DB2 as scheduled.

## 6.2.3 Using MySQL Replication in Web NMS

- Overview
- Prerequisites
- High-level Workflow
- Different Failover Scenarios
- Steps to Setup Replication
- Limitations
- Appendix

### Overview

One of the essential factors to determine the quality of a service is its availability. This is crucial in environments with mission critical applications. In Web NMS, the standby or the secondary server is one of the features that make the application scalable. Besides Web NMS failover, having a database failover ensures higher availability. With MySQL providing support for replication, the feature can be best used in Web NMS to optimize its availability and reduce the downtime.

### Prerequisites

Fair knowledge of database concepts.

### High-level Workflow

#### Setup

1. Primary back-end server, BE1 is connected to the database DB1
2. Secondary back-end server, BE2 is connected to the database DB2 (replicated database)
3. A front-end server, FE1 is connected to BE1.

#### Changes Effected in Web NMS

1. The secondary server, BE2 registers itself as standby with the primary server, BE1
2. The **database\_params.conf** file of the standby server, located in `<secondary_server home>/conf` directory, is copied to the primary server under the `<primary_server home>/conf/secondary` directory.
3. The same file is again transferred to all the FE servers connected to the primary server

<p><b>Note:</b> If you start a standalone front-end server after the primary and secondary servers are started, the following entry must be provided in the <code>DownloadFiles.xml</code> present in the <code>&lt;FE Home&gt;/conf</code> directory:</p>
--

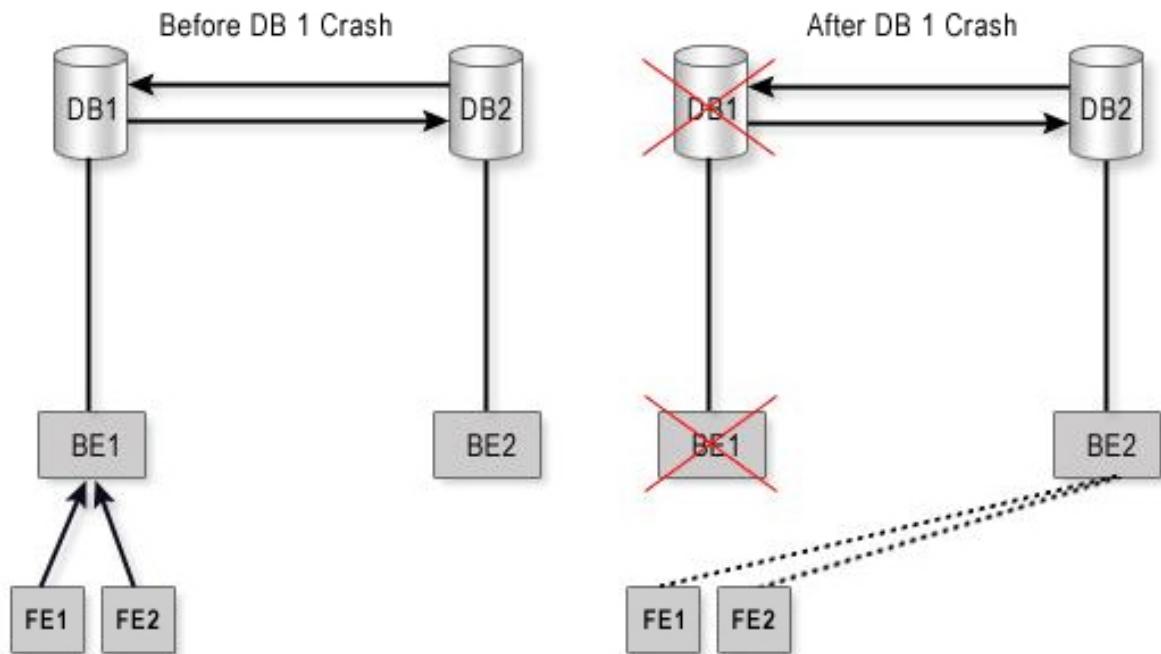
```

<SERVER-FILES downloadEachTime="true"/>
<FILE>.....</FILE>
<DIR>conf/secondary</DIR>
.....
<SERVER-FILES/>
```

## Reconnecting to Replicated Database

Database reconnection is supported in Web NMS. This feature is used in database replication to reconnect to the secondary database when the primary database goes down. For more details, refer to Accessing Connections section of our documentation:

1. The DB1 crashes.
2. BE1 connected to DB1 goes down with the message that connection to the database is lost.
3. The FEs connected to BE1 sense that it is down.
4. The database\_params.conf of BE2 is copied to the <FEs Home>/conf directory.
5. The FEs then re-connect to DB2.



## Different Failover Scenarios

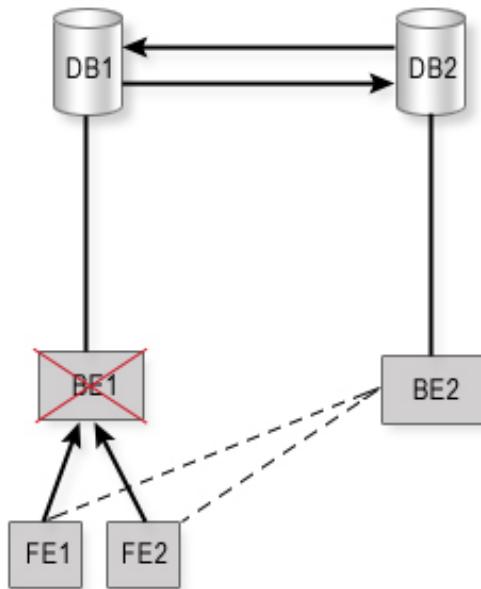
The above workflow is a scenario where the front-end servers reconnect to the secondary database. A few more situations are discussed below:

### 1. Setup Details

- o BE1 connected to DB1,
- o BE2 connected to DB2,
- o FE1, FE2 connected to BE1
- o Now, BE1 fails

**Action:** BE1 Fails|

**Result:** BE2 connected to DB2 takes over the functions of BE1 automatically and starts acting as the primary server. FEs connected to BE1 automatically re-connect to BE2.

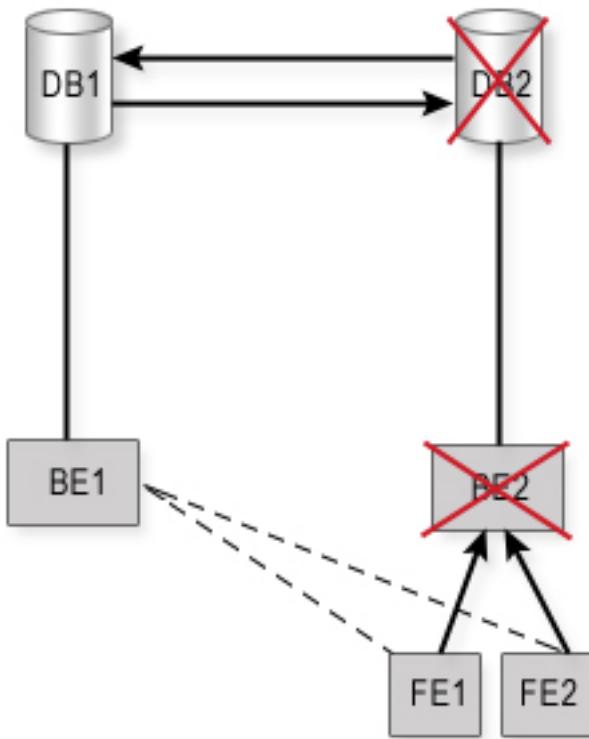


## 2. Setup Details

- BE2 is acting as primary and connected to DB2
- FE1, FE2 connected to BE2
- BE1 is up and running (now as a secondary server)
- Now, DB2 fails

**Action:** DB2 Fails

**Result:** BE2 is shut down saying that connection to the database is lost. BE1 takes over again and starts acting as the primary server. FEs connected to BE2 again reconnect to BE1.

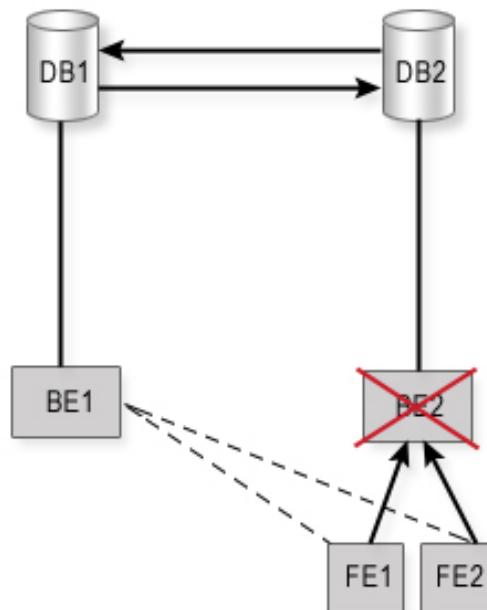


### 3. Setup Details

- BE2 is acting as primary and connected to DB2
- FE1 and FE2 connected to BE2
- BE1 is up and running (now as a secondary server)
- Now, BE2 fails

**Action:** BE2 Fails

**Result:** BE1 takes over the functions of BE and starts acting again as the primary server. The FEs will reconnect to BE1.



## Steps to Set up Replication

To use the MySQL database replication feature in Web NMS, you need to first set up replication in MySQL, and then make the corresponding configuration changes in Web NMS. The details are listed below:

### 1. Replicating MySQL:

The replication feature in MySQL enables copying of databases from one MySQL server to another. One database server acts as a **Master** and the other as a **Slave**. In Web NMS, two-way database replication is used, where it is like chained replication servers. That is, the Master and the Slave act as each other's Master and Slave.

To set up two-way replication in MySQL, follow the steps given in the following document:

[http://dev.mysql.com/doc/mysql/en/Replication\\_HOWTO.html](http://dev.mysql.com/doc/mysql/en/Replication_HOWTO.html)

<b>Note:</b> It is mandatory that you have to setup two-way replication, to use this feature in Web NMS.
--

### 2. Following are the configuration changes to be made in Web NMS. The changes must be effected both in BE1, and BE2.

- Configure the name of the host machine in which the MySQL server is installed, and the database name, in the configuration file database\_params.conf. This file is present in <Web NMS Home>/conf directory. This change must be made in both BE1 and BE2. Example entry in this file is given below:

`url jdbc:mysql://<host name>/<database name> AppModules`

Here <host name> is the name of host machine where MySQL is installed and <database name> is the name of the database.

- Configure the following two parameters in the configuration file serverparameters.conf, present in the <Web NMS Home>/conf directory:

**ENABLE\_DB\_RECONNECTION true**

**DB\_REPLICATION true**

After the above setup is ready, start the primary and secondary servers. Before that ensure that both, the Master and Slave databases are running.

## Limitations

- When configuring the database\_params.conf, ensure to provide only the actual DNS Name, or the IP Address of the host machine where the MySQL server is installed, even if it is the local host. **Do not** provide the host name as 'localhost' in this file.
- The number of transaction/non-transaction connections specified in the database\_params.conf must be the same in the primary and the secondary Web NMS servers (BE1 and BE2). This is because when database\_params.conf file is overwritten during database failover, only the URL is parsed and set to the ConnectionPool class. The values of the remaining parameters are assumed to be the same.

## Appendix

### From MySQL

- Replication FAQ
- Troubleshooting Tips
- SQL Queries for Master Server
- SQL Queries for Slave Server

### From Web NMS Documentation

Accessing Connections

## 6.3 Discovering Your Network

Web NMS automatically discovers your network and the elements in the network. The complete discovery process is governed by various configuration files located in the <Web NMS Home>/conf directory. The **seed.file** / **tl1seed.file** / **corbaseed.file** conf file located in the <Web NMS>/conf directory plays pivotal role in the discovery mechanism. The various parameters specified in the seed file determine the speed and efficiency of the discovery process.

This chapter explains configurations that can be made in the seed file using **Discovery Configurator** and also other discovery-related administrative tasks.

This chapter explains

---

- Using Discovery Configurator
  - Device and Network Discovery Options
  - Configuring Discovery Filters
  - ManagedObject UI Settings
  - Setting User Privileges
  - Configurable Discovery Parameters
-

## 6.3.1 Using Discovery Configurator

The discovery process can be configured to force the discovery of remote networks/nodes or to prevent the discovery of specific networks/nodes/local network. This is done using the configuration file **seed.file** in the <Web NMS Home>/conf directory, using APIs or using Web NMS Client. On startup, NMS Server will read the seed.file and get the configurations that are made in that file.

Configuring the discovery process manually by editing the seed.file/tl1seed.file is complex and error prone. Discovery Parameters can be configured at runtime through the runtime configuration wizard which updates the seed.file.



**Note:** This section explains how discovery service can be configured using the Discovery Configurator tool. To learn about the seed.file tags and parameters, refer to **example\_seed.file**, **example\_tl1seed.file** and **example\_corbaseed.file** located in the <Web NMS Home>/conf/examples directory. These configuration files have adequate explanation on each of the tags and parameters.

- 
- Opening Discovery Configurator
  - General Configuration
  - Protocol Configuration
  - Network Specific Discovery
  - Device Specific Discovery
  - Criteria Based Discovery
-

### 6.3.1.1 Opening Discovery Configurator

The Discovery Configurator is available as a standalone tool and runtime administration tool.

#### To open standalone Discovery Configurator

- Invoke the **DiscoveryConfigurator** script file located in <Web NMS Home>/bin/admintools directory.

#### To open the runtime Discovery Configurator

- In the Web NMS Client, from **Tools** menu, choose Runtime Administration. The **Runtime Administration** tool is displayed.
- From the **Categories** drop-down box or tree, choose **Topology > Discovery Configurator**. The Discovery Configurator tool is displayed.

#### Differentiating Standalone and Runtime Discovery Configurator

The basic functionality of the standalone Discovery Configurator and Runtime Administration UI Discovery Configurator remains the same except for the following factor.

**Standalone Discovery Configurator:** The configurations made using this tool during runtime will change the entries in **seed.file**, but the configuration will NOT take effect at run time. Only on subsequent restart of the server, the **seed.file** is read and the configurations are effected.

**Runtime Discovery Configurator:** The configurations made using this tool will take effect in the **seed.file** entries when the configured changes are effected. For instance, if the IP address for discovering specific devices is configured, the corresponding tag in **seed.file** is updated once the specific device is discovered.



**Warning:** Always use Discovery Configurator to carry out configurations in **seed.file**. In case **seed.file** is manually configured, ensure that XML format is not violated as it will throw parse exceptions. In such an event, exception message is printed in logs and discovery engine will start with default seed configurations and also new **seed.file** will be overwritten with default configurations.

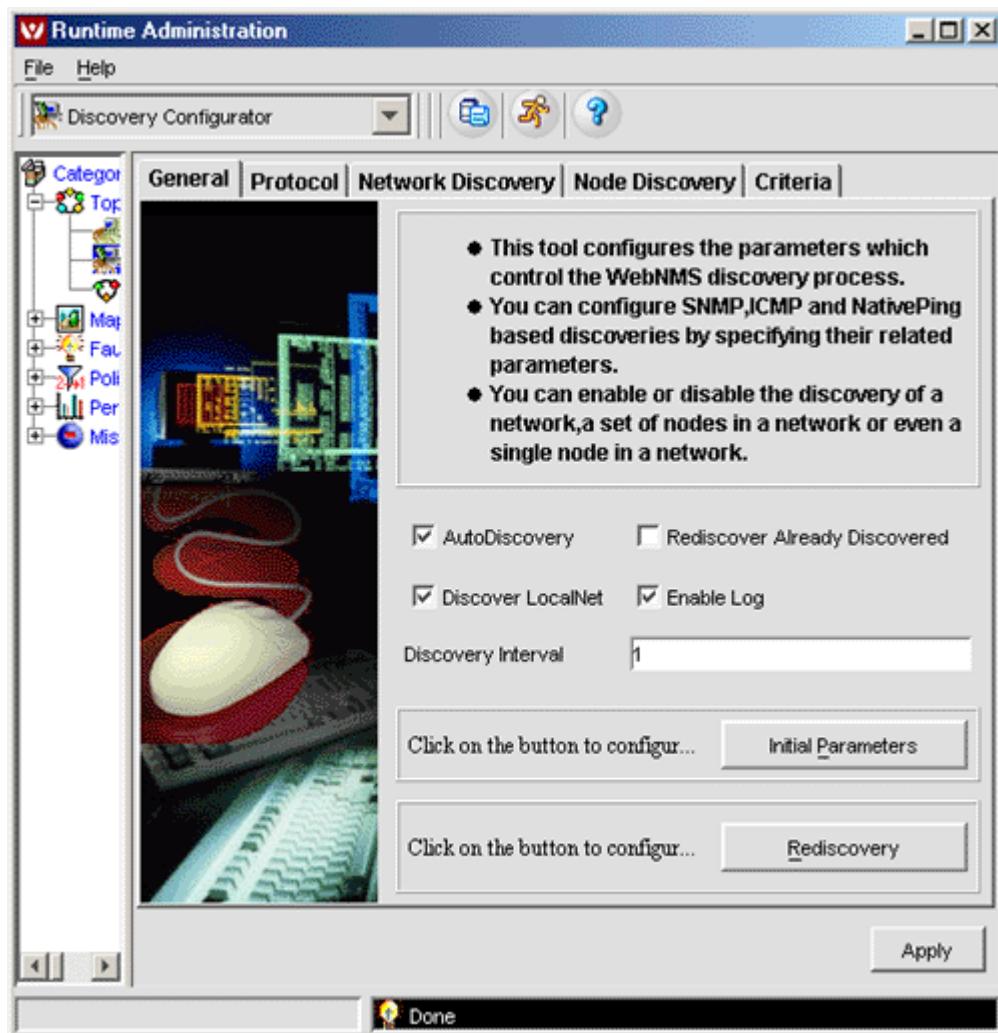


**Note:** NMS Server will read the **seed.file** during the restart of the server even if the database is not reinitialized.

### 6.3.1.2 General Configuration

The options explained in this topic are available in the **General** tab of the Discovery Configurator.

- Enabling/Disabling Auto-discovery
- Rediscovering already Discovered Devices
- Preventing Local Network from Being Discovered
- Logging Debug Messages
- Setting Discovery Interval
- Configuring Initial Discovery
- Scheduling Rediscovery



## Enabling/Disabling Auto-discovery

By default, the discovery process is automatically initialized when Web NMS Server is started.

To disable auto-discovery

1. In the **General** tab of the Discovery Configurator, deselect **AutoDiscovery**. By default, this option is enabled.
2. A warning message is displayed. Click **Yes** to disable auto-discovery.
3. Click **Apply** or from **File** menu, choose **Save Changes**.

Disabling this option will stop discovery process, i.e., auto-discovery will not happen when Web NMS Server is started. If you disable and then re-enable the AutoDiscovery option without shutting down or restarting the server, the discovery engine will just proceed with the rediscovery process according to the values set for the parameters, and there will not be any change in the already specified parameters.

## Rediscovering already Discovered Devices

By default, the rediscovery process discovers only devices that were not discovered previously. It does not rediscover the already discovered devices.

To rediscover already discovered devices

1. In the **General** tab of the Discovery Configurator, click **Rediscover Already Discovered**. By default, this option is disabled (not selected).
2. Click **Apply** or from **File** menu, choose **Save Changes**.

When the discovery process reschedules itself, based on the rediscovery interval specified, enabling or disabling this field decides the functionality of the discovery process. By default, this option is disabled. If enabled, during rediscovery, all the devices (discovered and undiscovered) will be rediscovered.

	<b>Note:</b> The above parameter does not control the behavior for DHCP nodes. DHCP nodes will be rediscovered every time and the objects in the database are updated with the latest information.
--	--

## Preventing Local Network from Being Discovered

By default, the local network and all its nodes are discovered. You can prevent the discovery of local network using the Discover LocalNet option.

To prevent local network discovery

1. In the **General** tab of the Discovery Configurator, deselect **Discover LocalNet**. By default, this option is enabled.
2. Click **Apply** or from **File** menu, choose **Save Changes**.

## Logging Debug Messages

By default, detailed discovery-related debug messages are logged in discoveryLogs.txt file located in the <Web NMS Home>/logs directory.

### To disable/enable logging of debug messages

1. In the **General** tab of the Discovery Configurator, select/deselect **Enable Log**. By default, this option is enabled.
2. Click **Apply** or from **File** menu, choose **Save Changes**.

## Setting Discovery Interval

The interval between discovery of two devices in the network can be controlled using the Discovery Interval option. The value set for this parameter determines the performance (CPU utilization and network traffic) of the discovery process.

### To set the discovery interval

1. In the **General** tab of the Discovery Configurator, enter the interval value (in seconds) in **Discovery Interval**. The value can be greater than or equal to zero and the default value is **1** second.
2. Click **Apply** or from **File** menu, choose **Save Changes**.

## Configuring Initial Discovery

**Initial discovery** process is the first discovery process that is started as soon as the Web NMS server is started (cold start or warm start). The configurations set here determine the speed of the initial discovery process. It is not mandatory to set the values for all the parameters.

This configuration applies only to the initial discovery process. For subsequent discoveries, the configuration values provided in General tab are used. When no parameters are set in the Initial Parameters section, Web NMS, by default, takes up the values set for the parameters in General tab, which is applicable both to the initial discovery process and for the subsequent discoveries.

### To set initial discovery parameters

1. In the **General** tab of the Discovery Configurator, click **Initial Parameters**. The **Initial Parameters** dialog box is displayed.
2. Enter the required values and click **OK**.
3. Click **Apply** or from **File** menu, choose **Save Changes**.

	<p><b>Tip:</b> Setting a value "0" to Discovery Interval option present in Initial Parameters dialog box is preferable, because these entries set in Initial Parameters are considered during the first start of the Web NMS server. During the successive rediscovery processes, the entries that are provided under the Discovery Interval (in General Configuration) and Native Ping options for the corresponding discovery parameters are taken into consideration. Hence, set "0" for Discovery Interval in Initial Parameters and give "1" or "2" for Discovery Interval in General Parameters.</p>
--	--

The options available in **Initial Parameters** are tabulated below:

Parameter	Description
<b>Discovery Interval</b>	Interval (in seconds) between the discovery of any two devices in the network.  <b>Default value:</b> 1 second
<b>Rediscovery Interval</b>	Interval (in hours) between two complete discoveries of a network.  <b>Default value:</b> 24 hours If a negative value is given, it is replaced by 24.
<b>ICMP Ping Retries</b>	Number of ICMP ping retries (status polling). This is used while pinging to discover the network.  <b>Default Value:</b> 0 (i.e., retry is performed only once)  If you set the value as 1, then retry is done twice. Setting this value at minimum gives better performance.
<b>SNMP Timeout</b>	Threshold value, in seconds, for all the SNMP requests.  This value is the maximum time that the requesting process waits for the first response, before attempting a retransmission.  It is useful when the discovery engine is discovering a remote network where the response time could be more.  <b>Default value:</b> 2 seconds  This value grows exponentially for each retries. This value is doubled for each retry. For example, if the timeout value is set to 5 seconds and retries set as 2, the first retransmission will happen after 5 seconds. The second after 15 seconds and so on.
<b>SNMP Retries</b>	Number of SNMP retries for discovery, status polling, and data collection.  <b>Default value:</b> 0 (i.e., retry is performed only once)  If you set the value as 1, then retry is done twice. Setting this value at minimum gives better performance.
<b>NativePing Timeout</b>	Threshold value for Native Ping.  <b>Default value:</b> 1 second
<b>NativePing Retries</b>	Number of retries for Native Ping.  <b>Default value:</b> 1 second

## Scheduling Rediscovery

The scheduled interval (in hours) between two complete discoveries of the networks can be configured. When pinging all the IP addresses in a network is finished, it waits for the specified time before starting the rediscovery of the networks.

You can schedule the rediscovery process by specifying the rediscovery interval in hours. The rediscovery process can also be configured to run at a specific hour on a specified date of the month or specified day of the week.

You can set the Rediscovery Interval using one of the following options:

1. Regular Interval option
2. Specific Dates option
3. Days of Week option

#### To set the rediscovery at Regular Interval

The time interval between two complete discovery of networks can be configured using the Regular Interval option. When regular time interval for rediscovery is configured (say 'x' hours), the Web NMS discovery engine, after discovering the IP Addresses in the network, waits for the specified 'x' number of hours before starting to rediscover the network again.

1. Click **General** tab in the Discovery Configurator.
2. Click **Rediscovery**. The **Rediscovery Scheduler** dialog box is displayed.
3. Click the **Regular Interval** option.
4. Specify the rediscovery interval in Hours, Minutes, and Seconds (as required). By default, the interval is set as **24** hours. You can set any value from 1 to 24 in the hours field. When you specify -1, rediscovery will be based on the entries configured in the **User's Schedule UI** option. When you give a negative value other than -1, the rediscovery interval will be taken as **24**.
5. Click **OK**.

For example, if you have set the interval at 6 hours, after the initial discovery, Web NMS starts rediscovery after 6 hours.

	<b>Note:</b> If the Rediscovery Interval is set using Regular Interval option, then the values set for Specific Dates and Days of Week options will not take effect.
--	--

To set rediscovery on specific dates

1. Click **General** tab in the Discovery Configurator.
2. Click **Rediscovery**. The **Rediscovery Scheduler** dialog box is displayed.
3. Click the **Specific Dates** option.
4. To choose a specific **date** on which rediscovery occurs, click the appropriate date option:
  - **All Dates:** Selects all the dates of a month and indicates rediscovery occurs every day.
  - **Specific Dates:** Constitutes a range of days. For example, if you select 5 and 15, then the rediscovery will take place from the 5th to 15th of every month.

When a particular month does not have the specified date, the rediscovery will occur based on the number of days difference between the current month and the next month. For example, if the specified date is 31 and the current month is October. As per this configuration, the rediscovery should occur after a range of 31 days. But the next month November does not have 31. In this case, rediscovery will be scheduled on 1st December (i.e., current month date 31 + specified date[31]). This is because all these calculations are in terms of milliseconds. Similarly if the date is specified as 31 and the current month is February (28 days), then the rediscovery is scheduled on 3rd March.

5. Select one of the **Hour** options:
  - **All Hours:** Selects all the hours in a day.
  - **Specific Hours:** Selecting a specific hour in day.
6. Click **OK** after you select the option.

#### To set rediscovery on specific days

1. Click **General** tab in the Discovery Configurator.
2. Click **Rediscovery**. The **Rediscovery Scheduler** dialog box is displayed.
3. Click the **Days of Week** option.
4. To choose a specific **day** on which rediscovery occurs, click the appropriate day option:
  - **All Days:** Selects all the days of the week.
  - **Specific Days:** Selecting specific days of the week. For example, if you select **Tue** and **Fri**, the rediscovery occurs only on those days, every week.
5. Select one of the **Hour** options:
  - **All Hours:** Selects all the hours in a day.
  - **Specific Hours:** Selecting a specific hour in day.
6. Click **OK** after you select the option.

#### Note:

- When both dates and days are configured, then the precedence is given to dates and not weekdays.
- When the dates or days is configured, the rediscovery interval is set as **-1** the **User's Schedule**.
- If the **Hour** field is not specified, **10** will be assigned as the default value. So, if you specify only the days or dates without specifying the hours, rediscovery will happen at the 10th hour of that particular day or date.

Combination of configurations that you can effect for rediscovery interval are listed in the table given below [based on seed.file configuration]:

When do you want rediscovery to take place?	Rediscovery Interval	Hour	Dates	Days
Default	24	Any entry specified here will not take effect	Any entry specified here will not take effect	Any entry specified here will not take effect
Particular Hour(s)	-1	Desired hour	No value should be configured	No value should be configured
Particular Day for every week	-1	No value should be configured	No value should be configured	Desired days
Particular Date for every month	-1	No value should be configured	Desired dates	No value should be configured
Particular Hour on a Particular Day	-1	Desired hour	No value should be configured	Desired day
Particular Hour on a Particular Date	-1	Desired hour	Desired date	No value should be configured

### 6.3.1.3 Protocol Configuration

All devices or network elements do not support the same protocol. The discovery process identifies the device and the protocol it supports and processes based on these parameters.

The **Protocol** screen of Discovery Configurator helps you configure the following:

- SNMP Protocol
- ICMP
- Native Ping
- TL1 Protocol

#### Configuring SNMP Protocol

##### To configure SNMP Properties

1. Click the **Protocol** tab in the Discovery Configurator.
2. Click **SNMP**.
3. Click **Properties**. The **SNMP Properties** dialog box is displayed.
4. You can configure the properties listed in the table below.
5. Click **OK**.

Option	Description
<b>SNMP Discovery</b>	Select this check box to enable or disable SNMP-based discoveries. By default, SNMP discovery is enabled.
<b>SNMP Retries</b>	Specify the number of retries to be made to query a device. <b>Default value:</b> 0 (i.e., only one attempt is made to query a particular node)
<b>SNMP Timeout</b>	Specify the timeout (in seconds) to wait for the first response before attempting a retransmission. <b>Default value:</b> 2 seconds.
<b>Read Community</b>	Specify a list of communities/community strings, such as private or public can be given to discover the devices when an SNMP request is given. Multiple values can be given separated by space. <b>Default value:</b> public
<b>Write Community</b>	Specify the community; such as private or public to set the write community property for all SNMP-enabled devices. <b>Default value:</b> public
<b>SNMP Ports</b>	Specify the ports while trying to communicate to the SNMP agents on each node. Multiple ports can be specified either as space-separated values or as a range of values. <b>Example:</b> 161 8001-8005 9099.

#### SNMPv3 Discovery

In Web NMS, discovery of SNMPv3 devices are performed in the following three ways:

1. SNMPv3 discovery for all the devices to be discovered
2. SNMPv3 discovery for specific networks to be discovered
3. SNMPv3 discovery for specific devices to be discovered

##### 1. SNMPv3 discovery for all the devices to be discovered

1. In **SNMP Properties** dialog box, select **SNMPv3 Discovery**.
2. Enter the **User Names** that are to be queried as comma-separated values.
3. Enter the common **Context Name** (only one value).
4. Ensure to set the values for **SNMP\_Ports**.
5. Click **OK**.

The three ways of SNMPv3 device discovery have a precedence of execution. If you have configured all the three ways of discovering SNMPv3 devices, then the order of precedence is as follows.

1. Initially, the Network-specific discovery is performed
2. Then the Device-specific discovery is performed.
3. Finally, the discovery of all devices (as configured in this dialog box) is performed.

## Configuring ICMP

### To configure ICMP properties

1. Click the **Protocol** tab in the Discovery Configurator.
2. Click **ICMP**.
3. Click **Properties**. The **ICMP Properties** dialog box is displayed.
4. You can configure the properties listed in the table below.
5. Click **OK**.

Options	Description
<b>ICMP Discovery</b>	Enable/disable ICMP discovery using the ICMP Discovery option. By default, ICMP discovery is enabled.
<b>Ping Retries</b>	Specify the number of ping retries to be made. <b>Default value:</b> 0 (i.e., ICMP Ping is performed only once).
<b>Ping Timeout</b>	Specify the time (in seconds) for the server to wait for the request from host. <b>Default value:</b> 1

## Configuring Native Ping

### To configure Native Ping properties

1. Click the **Protocol** tab in the Discovery Configurator.
2. Click **NativePing**.
3. Click **Properties**. The **Native Ping Properties** dialog box is displayed.
4. You can configure the properties listed in the table below.
5. Click **OK**.

Options	Description
<b>Native Ping Timeout</b>	Specify the timeout value for Native ICMP Ping. <b>Default value:</b> 2
<b>Native Ping Retries</b>	Specify the number of retries for Native ICMP Ping. <b>Default value:</b> 2
<b>Native Ping Sweep Packets</b>	Specify the number of packets for Native ICMP Ping. <b>Default value:</b> 10
<b>Native Ping Sweep Sleep Interval</b>	Specify the time interval between two Native ICMP Pings. <b>Default value:</b> 2
<b>Native Ping Debug Level</b>	Specify the debug level for Native ICMP Ping. <b>Default value:</b> 1
<b>Native Ping Sweep</b>	A ping sweep is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts (computers).  Enable/disable native ping sweep using this option. By default, it is disabled.

The parameters configured in this **Native Ping Properties** dialog box are the default parameters that are written automatically during Web NMS Server startup, if the existing entries in the **seed.file** are removed. Native ping (code written in C) is used to ping (perform ICMP ping) for devices. Native ping is used to improve the performance, over the default system ping.

Native Ping can be enabled or disabled using **serverparameters.conf** or the startup options in **startnms.bat/sh** files. By default, it is enabled for Windows alone. Here, **startnms.bat/sh** file entries will override the values specified in **serverparameters.conf**.

## Configuring TL1 Protocol

The configurations made in this dialog box are written to the **tl1seed.file** located in the <Web NMS Home>/conf directory. All parameters configured in the **tl1seed.file** are stored as properties of the ManagedObject.

### To configure TL1 Protocol Properties

1. Click **Protocol** tab in the Discovery Configurator.
2. Click **TL1**.
3. Click **Properties**. The **TL1 Properties** dialog box is displayed.
4. Click **Add** to add device groups. The **GroupPropertiesDialog** dialog box is displayed. The fields in this dialog box is explained in the following table. On configuring the parameters, click **OK**.
5. Click **IP List** to view the IP list configured to the device group you have added. In this view, click **Add** to add IPs to the device group.
6. Click **GNE List**. The **GNEPropertiesDialog** dialog box is displayed which lists the GNEs configured to the device group you have added.

Click **Add** to add GNEs to the device group. The **GNE IP, Port** (Terminal Server Port), and **Connection Handler** (enter com.adventnet.nms.topodb.tl1.TL1BlankConnHandler, which is the default implementation or enter your own implementation of the Connection Handler) are mandatory fields.

Click **TID List** to view the TID properties for the selected GNE. Click **Add** to add TID properties for the selected GNE. The **TidPropertiesDialog** dialog box is displayed. The **TID Name, Type**, and **Connection Handler** (enter com.adventnet.nms.topodb.tl1.TL1BlankConnHandler, which is the default implementation or enter your own implementation of the Connection Handler) are mandatory fields.

7. Click **Delete** to delete a device group.
8. Click **Modify** to modify an existing device group.
9. Click **Save** to save the additions/modifications made to the device groups.

## Hierarchical Configuration Feature

In the **tl1seed.file**, you configure a lot of information related to the device discovery, status polling, etc. To ease the burden of configuring each of those fields for each TL1 device, a hierarchical configuration facility is provided in the **tl1seed.file** using Discovery Configurator.

The hierarchy is :

**GLOBAL (TL1DISCOVERY) --> DEVICE GROUP (GROUP) --> DEVICE (IP)**

All the parameters and the commands can be configured at all the three levels. The parameters are searched at the IP level, which overrides the parameters mentioned in the Global and Group levels. If they are not mentioned at the IP level, then the parameters mentioned in the next immediate hierarchy, i.e., Group level, which overrides the parameters mentioned in the Global level, are inherited. If the parameters are not mentioned in the Group level also, then the parameters mentioned in the next immediate hierarchy i.e. Global level, are inherited.

Using this hierarchy, you can specify certain globally common parameters at the global level. These parameters are applied to all the TL1 devices configured under any device group. Whatever parameters you specify at the device group level correspond to those devices configured under that group and they override the parameters you specify at the global level. Parameters specific to a particular type of device can be specified at the device group level. You can specify the parameters specific to a particular TL1 device at the device level. These parameters override those parameter you have specified at the group level and the global level.

### 6.3.1.4 Network Specific Discovery

- Forcing Discovery of Remote Networks
- Discovering Range of IPs in a Network
- Configuring DHCP Support for Discovery
- Performing Network Specific Discovery of SNMP Devices
- Preventing Network Discovery
- Deleting Network Entries

#### Forcing Discovery of Remote Networks

The Web NMS discovery engine, by default, discovers all the networks (to which the management station running the Web NMS server is connected). It also adds any other network that it comes across (through router) to the topology and makes that network object unmanaged, which means no discovery will go on.

If you want to add a remote network and also perform discovery on that network, it can be done using the **Discover** option in the Discovery Configurator.

##### To enable discovery of remote networks

1. Click the **Network Discovery** tab in the **Discovery Configurator**.
2. Select **Discover**.
3. Select **Entire Network**.
4. Enter the network address in **IPAddress** and sub-netmask of the network in **Netmask**.
5. Click **Add**. The IP Address and Netmask is added to the screen with the **Discover** column enabled (checked), that is, discovery of those remote networks is enabled. Multiple networks can be configured by adding more IPAddresses and NetMask.

#### Discovering Range of IPs in a Network

##### To discover only a range of ipaddresses in a network

1. Click the **Network Discovery** tab in the **Discovery Configurator**.
2. Select **Discover**.
3. Select **Set of Nodes**. The **Start IP** and the **End IP** text boxes are enabled.
4. Enter the network address in **IPAddress** and sub-netmask of the network in **NetMask** fields.
5. Enter the starting IP address and the ending ipaddress in the range of ipaddresses to be discovered in **Start IP** and **End IP** respectively.
6. Click **Add**. Multiple Range of ipaddresses in a single network can also be configured.



**Note:** The range of IPs specified here will not be discovered and added, if any of the node properties is specified in the Disallow Criteria. Hence, ensure that the properties of the IPs specified here are not specified in the Disallow Criteria.

## Configuring DHCP Support for Discovery

### To enable DHCP support

1. Click the **Network Discovery** tab in the **Discovery Configurator**.
2. Select **Discover**.
3. Select **Set of Nodes**. The **Start IP** and the **End IP** text boxes are enabled.
4. Enter the network address in **IPAddress** and sub-netmask in **NetMask** fields.
5. Enter the starting IP address and the ending ipaddress in the range of ipaddresses to be discovered in the **Start IP** and the **End IP** respectively.
6. Select **DHCP**. Only when the **Start IP** and the **End IP** are given with the **DHCP option disabled**, will that particular range of network get discovered. But if Start IP and End IP are specified with **DHCP option enabled** then the nodes in that particular range will be discovered as DHCP Nodes and other nodes will also be discovered as Non-DHCP nodes.
7. Click **Add**.



**Note:** Discovering/pinging only the devices specified in the range when DHCP is enabled is not supported in Web NMS.

### Example:

When you want to discover devices that support DHCP in a network "129.253.229.0", wherein you know only the range of IP addresses from 129.253.229.100 to 129.253.229.150 which are in the DHCP range,

1. Enter the IPAddress as 129.253.229.0
2. Enter the NetMask as 255.255.0.0
3. Enter the Start IP as 129.253.229.100
4. Enter the End IP as 129.253.229.150
5. Enable DHCP option

The above entry will discover and add the nodes with the range 129.253.229.100 to 129.253.229.150 with the "DHCP" enabled. This will also add all the other nodes in the network 129.253.229.0 with *DHCP* disabled.

## Performing Network Specific Discovery of SNMP Devices

Web NMS discovery module facilitates discovering the SNMP (v1, v2c, and v3) devices in a specific network or a range of devices in a network.

### Discovering SNMP (v1 and v2c) devices with specific Community and Port in a network

The Web NMS discovery engine, by default, uses the community string public and the agent port 161 while discovering SNMP devices. But some devices in the network could use a different port and community.

### To discover those devices in a particular network

1. Click the **Network Discovery** tab in the **Discovery Configurator**.
2. Select **Discover**.
3. Select **SNMP**.
4. Click **SNMP Properties**. The **Snmp Properties** dialog box is displayed.

5. Click **V1** or **V2** version as required. The **SNMP Properties** panel is enabled.
6. Enter the community of the node in **Community** field.
7. Enter the port in **SNMP Agent Port** field.
8. Click **OK**.
9. Save this configuration in the Discovery Configurator.

On performing this, the discovery engine discovers those SNMP devices in the specified network with the configured community and port.

## Discovering SNMPv3-Enabled Devices in a Network

SNMPv3 discovery for specific networks is useful under the following two situations:

**a)** When only certain network has SNMPv3 devices, sending v3 queries for all the networks to be discovered would be redundant. Hence, only specific networks should be configured for v3 discovery. The following are the configurations to be made for this situation.

1. Disable **SNMPv3 Discovery** option in **SNMP Properties** dialog box.
2. Click **Network Discovery** in the **Discovery Configurator**.
3. Select **Discover** and specify the **IPAddress** and **NetMask** of network that should be discovered as v3.
4. Select **SNMP** and click **SNMP Properties**. The **Snmp Properties** dialog box is displayed.
5. Select **V3**. The **SNMP V3 Properties** panel is enabled.
6. Click **Add**. The **SNMP V3 Properties** dialog box is displayed.
7. In the **General** tab enter the security user name, context name and the port number in the **User Name**, **Context Name**, and **Agent Port** fields respectively.
8. In the **Security** tab, select the security level from **Security Level** combo box. Enter the authentication protocol name and authentication password in **Auth Protocol** and **Auth Password** fields respectively. For **AuthPriv** security level, enter the privacy protocol and privacy password in **Priv Protocol** and **Priv Password** field respectively.
9. Click **OK**.
10. Click **Add**.

In this setup, the discovery engine will send SNMP v3 queries only to the specific networks or set of nodes that are configured. If the v3 queries to devices in the specific network fail, then v2 and v1 queries are sent to the devices. If any of these succeeds, the device will be added with to appropriate version set to it.

**b)** Also for a particular network, if the common **username** and **contextname** specified should not be used and you want to override the common configurations specified for this network, you can use this network-specific SNMP configuration. The configurations to be made for this situation are:

1. Enable **SNMPv3 Discovery** option and give the **User Names**, **Context Name**, and **SNMP\_Ports** in the **SNMP Properties** dialog box.
2. Click **Network Discovery** in the **Discovery Configurator**.
3. Select **Discover** and specify the **IPAddress** and **NetMask** for the network whose v3 configurations should be overridden.
4. Select **SNMP** and click **SNMP Properties**. The **Snmp Properties** dialog box is displayed.
5. Select **V3**. The **SNMP V3 Properties** panel is enabled.

6. Click **Add**. The **SNMP V3 Properties** dialog box is displayed.
7. In the Network Discovery dialog box, in the **General** tab, override the common configurations that you want.
  - For overriding user name, use User Name option
  - For overriding context name, use Context Name option
  - For overriding SNMP port, use Agent Port option
8. In the **Security** tab, select the security level from **Security Level** combo box. Enter the authentication protocol name and authentication password in **Auth Protocol** and **Auth Password** fields respectively. For **AuthPriv** security level, enter the privacy protocol and privacy password in **Priv Protocol** and **Priv Password** field respectively.
9. Click **OK**.
10. Click **Add**.

It is enough if you override the necessary properties alone. The values of those properties that are not specified in the **Network Discovery** tab will be taken from the common values.



**Note:** During discovery, sometimes the SNMPv3 devices are discovered as SNMPv2 devices. This occurs when the timeout or retries value is less. Hence to avoid this, set the SNMP Timeout or the SNMP Retries more than the default optimal value based on your agent's performance. These values can be configured in the Initial Parameters UI.

## Preventing Network Discovery

### To prevent the discovery of specific network

1. Click **Network Discovery** in the **Discovery Configurator**.
2. By default, the **Discover** option is selected. Disable (uncheck) this option.
3. Save the configuration.

This will prevent the network from being discovered and added to the topology database. Multiple networks can be prevented by adding more IP addresses and Netmasks.



**Note:** This tag will not add the specified network, even if the network is reachable from the host in which the Web NMS is running.

## Deleting Network Entries

In the **Network Discovery** tab of the **Discovery Configurator**, you can delete a network entry specified in it by clicking the **Delete** button. Deleting an entry in the Discovery Configurator, will not delete that network from the database. This will delete the entry for the network only in the **seed.file**. Hence, when you restart the server without reinitializing it, then that particular network will be discovered again as its entry is retained in the database. Similarly when the discovery engine is scheduled for rediscovery, that network will be rediscovered (if rediscovery is enabled ).

As the Discovery Configurator acts as a medium to put the entries in the seed.file, all modifications done using this tool will effect only in the seed.file and will not have an impact on the database.

### 6.3.1.5 Device Specific Discovery

The discovery mechanism enables you to force the discovery of specific devices or to discover devices with specific port and agent, before discovering any other devices in the network.

- Forcing Discovery of IP Addresses in a Network
- Discovering Nodes from Local Network (which is disabled)
- Discovering Parent Net
- Discovering SNMP Devices with Specific Community and Agent Port
- Discovering SNMPv3-Enabled Devices
- Preventing Discovery of IP Addresses in a Network

#### Forcing Discovery of IP Addresses in a Network

**To force the discovery of specific nodes** (before discovering any other device in the network)

1. Click the **Node Discovery** tab in the **Discovery Configurator**.
2. Select **Discover**.
3. Enter the IP address of the device that is to be discovered and netmask of the device in **IPAddress(es)** and **NetMask** fields respectively. Both these fields are mandatory.
4. Click **Add**. The IP Address and NetMask will be added to the table above the fields with the **Discover** column being enabled (checked), that is, discovery of those nodes are enabled. If it is unchecked then the node will be ignored/undiscovered. Multiple IP addresses can also be configured.



**Note:** If the network corresponding to the given address is not available in the topology database, then the discovery engine will first add the network object to the database and will discover the specified IP before adding any other node in the network.

#### Discovering Nodes from Local Network (which is disabled)

There is a provision to discover nodes from the local network, where the discovery of local network option is disabled. Refer to **Preventing local network from being discovered** in **General Parameters Configuration**.

**Example screen shots of Local Network being disabled and Node to be discovered configurations are shown below:**

**Discovery Configurator**

**Network Discovery** tab selected.

Description:

- This tool configures the parameters which control the WebNMS discovery process.
- You can configure SNMP, ICMP and NativePing based discoveries by specifying their related parameters.
- You can enable or disable the discovery of a network, a set of nodes in a network or even a single node in a network.

Checkboxes:

- AutoDiscovery
- Rediscover Alr...
- Discover LocalNet (highlighted with red border)
- Enable Log

Discovery Interval: 1

**Runtime Administration**

**Node Discovery** tab selected.

Configure Node Discovery parameters. IPAddress, Netmask, Community, Port, SNMP Version, UserName and ContextName are the key parameters for Node Discovery.

Discover	Parent ...	IPAddress	NetMask	Commu...	Port	Version	Us...	Co...
<input checked="" type="checkbox"/>	true	192.168.4.10	255.255.255.0	public	161	v1		

Checkboxes:

- Discover

Fields:

- IPAddress(es):
- NetMask:
- SNMP Version: v1
- Discover Parent Net:
- Community: public
- SNMPAgentPort: 161
- UserName:
- ContextName:

Buttons:

- Add
- Delete
- Modify
- Properties
- Apply
- Done

The above configuration can be performed to discover and add the local network and the node 192.168.4.10 (if the local network is 192.168.4.0 and is disabled).

## Discovering Parent Net

By default, when a device is discovered in the network, its parent network is also discovered, that is, other devices in that network is also discovered.

### To prevent discovery of parent network

1. Click the **Node Discovery** tab in the **Discovery Configurator**.
2. Select **Discover**.
3. Enter the IP address of the device that is to be discovered and netmask of the device in **IPAddress(es)** and **NetMask** fields respectively. Both these fields are mandatory.
4. Uncheck **Discover Parent Net**.
5. Click **Add**.

## Discovering SNMP Devices with Specific Community and Agent Port

By default, Web NMS discovery uses the community string **public** and the agent port **161** while discovering SNMP devices. But some devices in the network could use a different port and community.

### To discover SNMP devices with specific community and port

1. Click the **Node Discovery** tab in the **Discovery Configurator**.
2. Select **Discover**.
3. Enter the IP address of the device that is to be discovered and netmask of the device in **IPAddress(es)** and **NetMask** fields respectively. Both these fields are mandatory.
4. Choose the SNMP version **v1**, **v2**, or **v3** from **SNMP Version** drop-down box.
5. Enter the community of the device in **Community** field. Default value is **public**.
6. Enter the SNMP agent port of the device in **SNMPAgentPort** field. Default value is **161**.

## Discovering SNMPv3-Enabled Devices

SNMPv3 discovery for specific devices is useful under the following two situations:

**a)** In a network where only selected devices are SNMPv3 devices, sending v3 queries for all the devices would be redundant. Hence, only selective devices should be configured for v3 discovery. The following are the configurations to be made for this situation.

1. Click the **Protocol** tab in the **Discovery Configurator**.
2. Select **SNMP** and click **Properties**. The **SNMP Properties** dialog box is displayed.
3. Disable **SNMPv3 Discovery** if already enabled and click **OK**.
4. Click the **Node Discovery** tab in the **Discovery Configurator**.
5. Select **Discover**.
6. Enter the IP address of the device that is to be discovered and netmask of the device in **IPAddress(es)** and **NetMask** fields respectively. Both these fields are mandatory.
7. Choose **v3** from **SNMP Version** drop-down box.
8. Enter the security user name, context name and the port number in the **UserName**, **ContextName**, and **SNMPAgentPort** fields respectively.
9. Click **Properties**. The **SNMP v3 Properties** dialog is invoked.
10. Enter appropriate values in the fields available.

11. Click **OK**.

12. Click **Add**.

In this setup, the discovery engine will send SNMP v3 queries only to devices that are specified in the **IPAddress** with SNMP Version set as **v3**. If the v3 queries to these devices fail, then v2 and v1 queries are sent to the devices. If any of these succeeds, the device will be added to the appropriate version set to it.

**b)** Also for a particular device, if the common **username** and **contextname** specified should not be used and you want to override the common configurations specified for this device, you can use this device-specific v3 configuration. The configurations to be made for this situation are:

1. Click the **Protocol** tab in the **Discovery Configurator**.
2. Select **SNMP** and click **Properties**. The **SNMP Properties** dialog box is displayed.
3. Enable **SNMPv3 Discovery** if already disabled.
4. Enter the **User Name**, **Context Name**, and **SNMP\_Ports** and click **OK**.
5. Click the **Node Discovery** tab in the **Discovery Configurator**.
6. Select **Discover**.
7. Enter the IP address of the device (for those devices whose v3 configurations should be overridden) and netmask of the device in **IPAddress(es)** and **NetMask** fields respectively. Both these fields are mandatory.
8. Choose **v3** from **SNMP Version** drop-down box.
9. Override the common configurations by entering values for **UserName**, **ContextName**, and **SNMPAgentPort** fields.
10. Perform steps 9 to 12 as explained in previous section.

It is enough if you override the necessary properties alone. The values of those properties that are not specified in the **Node Discovery** tab will be taken from the common values.



**Note:** During discovery, sometimes the SNMPv3 devices are discovered as SNMPv2 devices. This occurs when the timeout or retries value is less. Hence to avoid this, set the SNMP Timeout or the SNMP Retries more than the default optimal value based on your agent's performance. These values can be configured in Initial Parameters.

## Preventing Discovery of IP Addresses in a Network

The discovery engine can also be configured to prevent the discovery of certain IP addresses in a network.

### To prevent the discovery of a device: Procedure 1

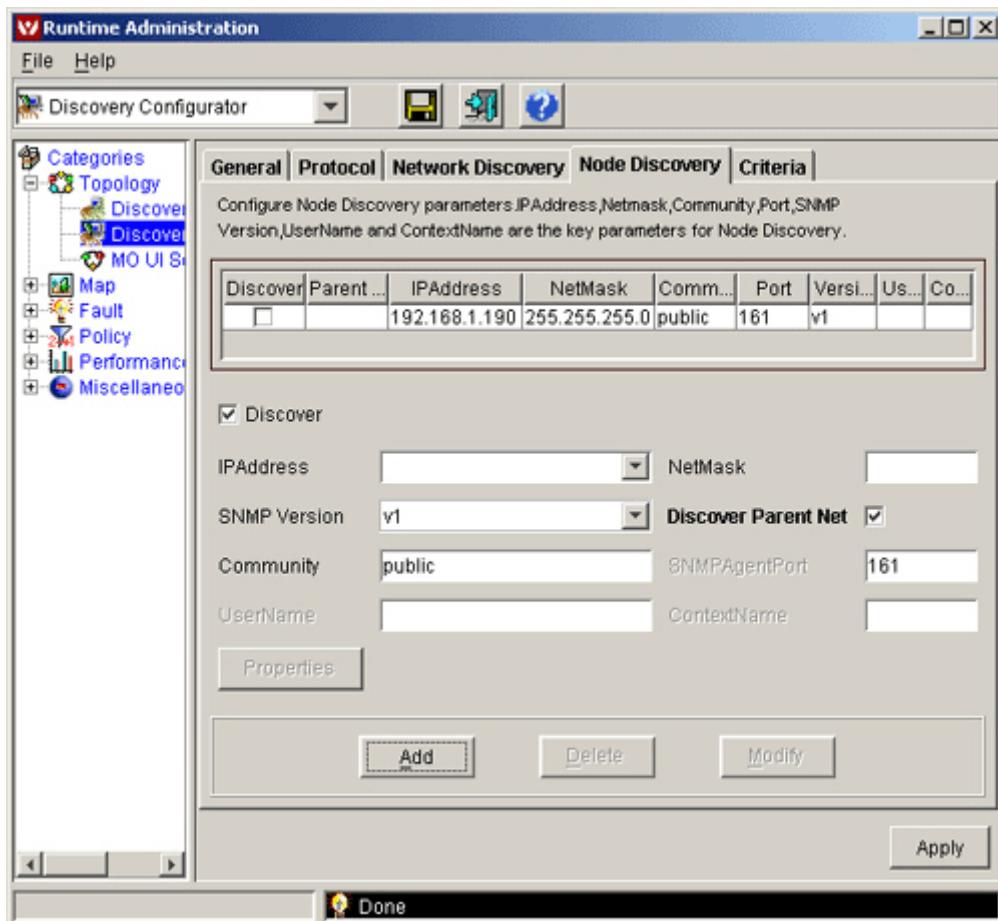
1. Click the **Node Discovery** tab in the **Discovery Configurator**.
2. Disable **Discover** (not selected).
3. Enter the IP address of the device (for those devices whose v3 configurations should be overridden) and netmask of the device in **IPAddress(es)** and **NetMask** fields respectively. Both these fields are mandatory.
4. Click **Add**.

### To prevent the discovery of a device: Procedure 2

This procedure is applicable only if the device is already configured and displayed in table above the fields.

1. Select the row that represents the required device in the table.

2. Disable **Discover** option.
3. Click **Modify**.



### 6.3.1.6 Criteria Based Discovery

To configure discovery based on Managed Object (MO) properties, the **Criteria** tab of the Discovery Configurator can be used. This configuration facility is used to allow or disallow the discovery of only those objects whose properties match with the specified match criteria.

The Allow Criteria option is to be enabled when only those objects which satisfy the specified criteria should be discovered. If it is unchecked, then only those objects which do not satisfy the specified criteria will be discovered.

The configurations made in Allow Criteria are equivalent to the AND operator and the Disallow Criteria is equivalent to the OR operator. When multiple properties are given in the Allow Criteria, the objects get discovered only if all the specified properties match with that of the incoming object. When multiple properties are specified in the Disallow Criteria, even if one of the properties matches with that of the incoming object, the object will not be discovered.



**Note:** Only the 'name', 'type', 'ipAddress', 'sysOID', and the 'isSNMP' attributes of the ManagedObject (and their derivatives) can be used with the Allow Criteria and Disallow Criteria specifications. Though others can be used, the behavior is neither tested nor guaranteed.

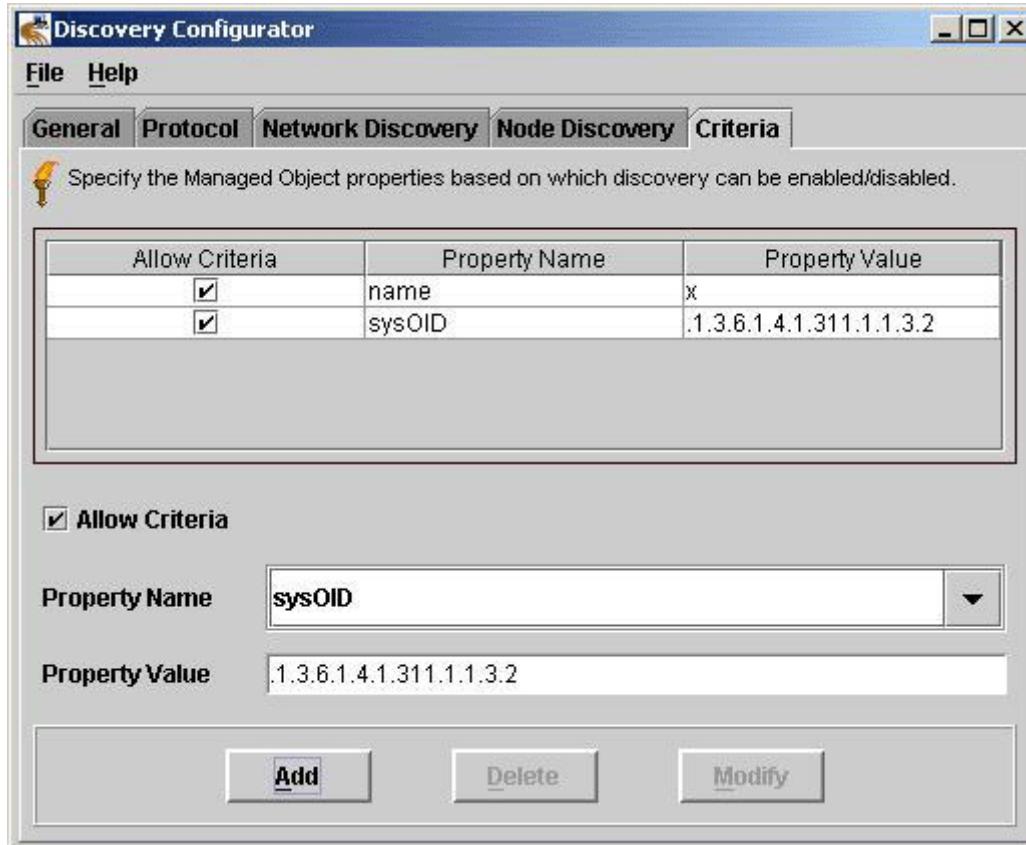
- Discovering Devices Only with Specific Properties
- Discovering Only SNMP Nodes
- Discovering Objects with Specific IP
- Discovering Objects with Multiple Properties
- Preventing Discovery of Devices with Specific Properties

#### Discovering Devices Only with Specific Properties

##### To discover devices with specific properties

1. Click the **Criteria** tab in the **Discovery Configurator**.
2. Select **Allow Criteria**.
3. Choose or enter the property from **Property Name** drop-down box. By default, five of the Managed Object Properties (name, type, ipAddress, sysOID, isSNMP) are available. The MO property name can be any of the fields in the ManagedObject class or one of its derived classes. Multiple values can be entered separated by space.
4. Enter the value for the property chosen in **Property Value** field.
5. Click **Add**. The property name and its respective value are added in the table above the fields.

**Example:** The following screen shot depicts the Allow Criteria set for a specific name and sysOID properties.



This will add only those objects whose names are x and sysOID property as .1.3.6.1.4.1.311.1.1.3.2. All other objects will be filtered out, i.e., all other objects will not be added to the database.

## Discovering Only SNMP Nodes

### To discover only SNMP nodes

1. Click the **Criteria** tab in the **Discovery Configurator**.
2. Select **Allow Criteria**.
3. Select **isSNMP** from the **Property Name** drop-down box.
4. Enter **true** in the **Property Value** field.
5. Click **Add**.

On performing this, only the SNMP nodes are discovered and added to the database. Ensure that the SNMP nodes are present and reachable from the host that runs the Web NMS server.

## Discovering Objects with Specific IP

### To discover only the object corresponding to a specific IP

1. Click the **Criteria** tab in the **Discovery Configurator**.
2. Select **Allow Criteria**.
3. Select **ipAddress** from the **Property Name** drop-down box.
4. Enter IP Address in the **Property value** text box.
5. Click **Add**.

## Discovering Objects with Multiple Properties

When multiple properties are specified as criteria, the objects are discovered only if all of the specified properties match with that of the incoming managed object.

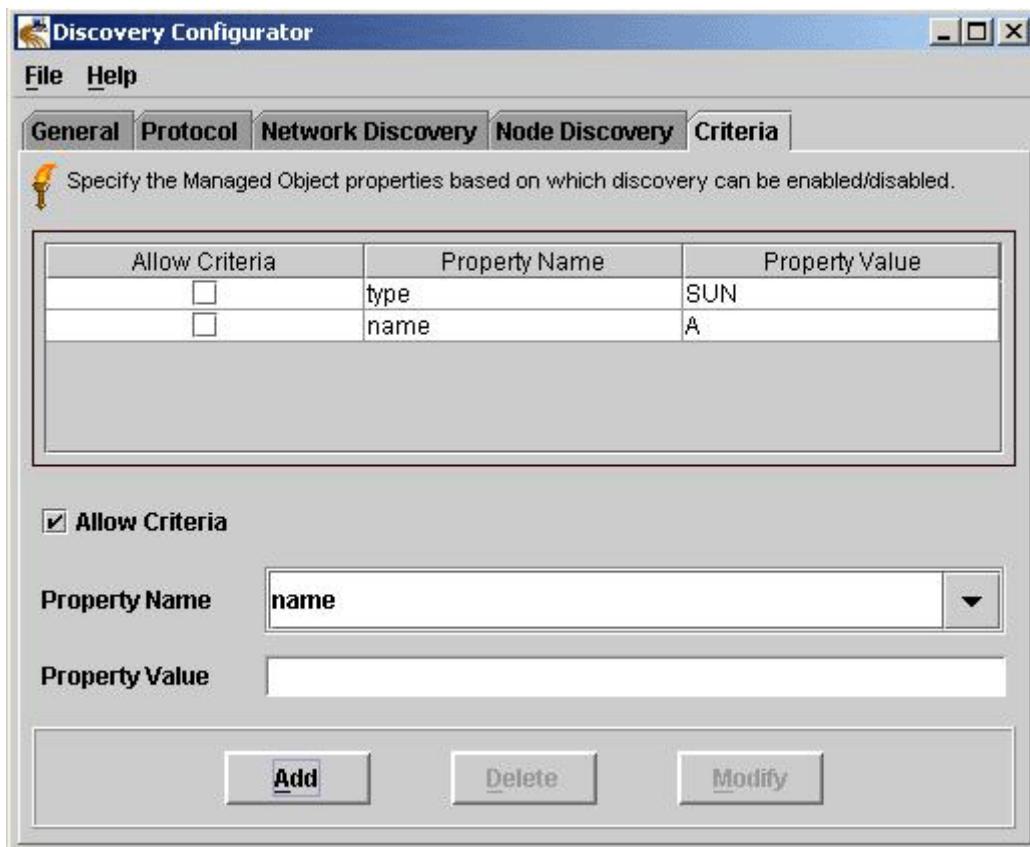
For example, if **isSNMP** is set "true", **SYSOID** is set ".1.3.6.1.4.1.311.1.1.3.2", and **type** is set "node", this configuration will discover all the SNMP node objects, whose poll interval is set as 300 seconds. Even if either of the properties does not match, the object will not be discovered.

## Preventing Discovery of Devices with Specific Properties

The discovery engine can be configured to prevent the discovery of devices with specific properties. You can either disable the already added criteria or enter new criteria with the **Allow Criteria** option disabled (unchecked).

### Example

When the value of properties **type** is set **SUN** and **name** set as **A**, discovery engine will prevent the discovery of devices whose type property is SUN and its name starts with the letter A. Even if either of the properties matches with the incoming managed object, the object will not be discovered. This example is depicted in the screen shot given below.



## 6.3.2 Device and Network Discovery Options

Networks and their elements are discovered automatically by Web NMS and the discovery process is carried out in a predetermined way. If you need to discover a network or node manually instead of waiting for Web NMS to discover it automatically, use the Add New Network and Add New Node options.

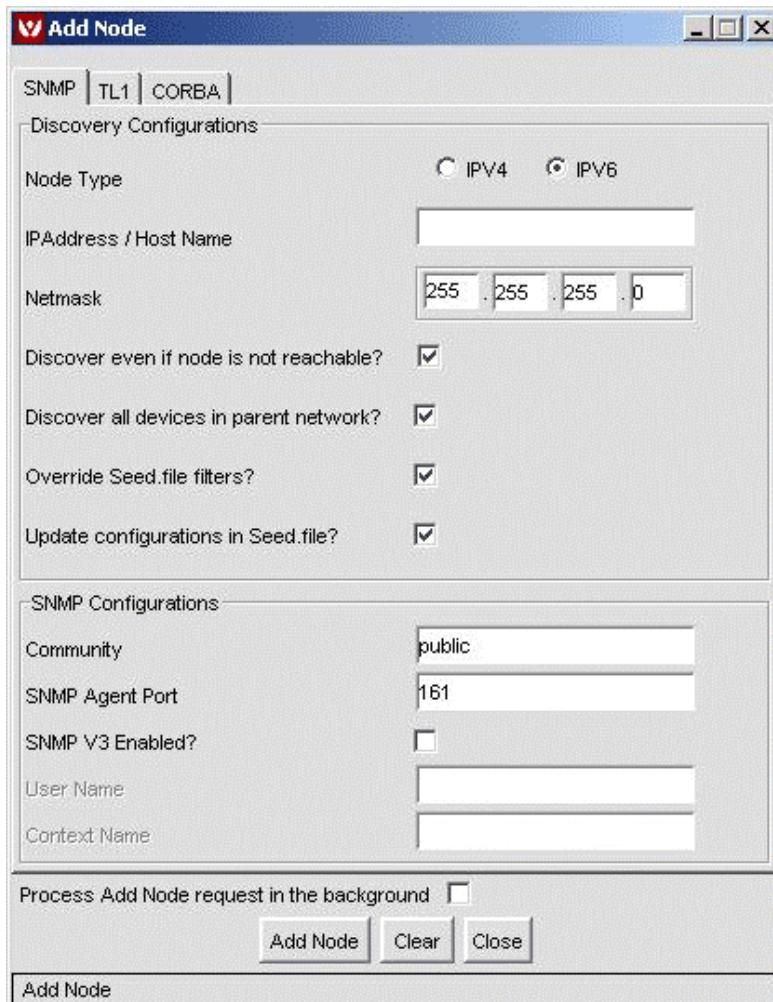
- Adding a Node
- Adding a Network
- Deleting Object and Traces
- Refreshing a Node

### Adding a Node

This section explains how you can manually add a node to the topology. There is separate provision to add SNMP, TL1, and CORBA devices.

To add a node

1. In the Web NMS Client, click **Network Database** on the left-side tree. The **Network Database** frame is displayed on the right.
2. From **Edit** menu, choose **Add Node**. The **Add Node** dialog box is displayed as below:



3. There are three tabbed panes **SNMP**, **TL1**, and **CORBA**. Select the required protocol tab that your device is based on and enter appropriate values for the input fields. For information on each of the fields in SNMP, TL1, and CORBA tabs, refer to the Appendix.

**Note:** The **TL1** Tab will be available only if the device Group entries are added in **tl1seed.file** located in the <Web NMS Home>/conf directory.

4. Click **Add Node**.

If the node IP that you have entered has already been added to the database and discovered by Web NMS, relevant message is displayed in the Add Node dialog box.

## Adding a Network

This section explains how you can manually add a network to the topology.

To add a network

1. In the Web NMS Client, click **Network Database** on the left-side tree. The **Network Database** frame is displayed on the right.
2. From **Edit** menu, choose **Add Network**. The **Add Network** dialog box is displayed.
3. Enter values in appropriate fields. For information on each of the fields, refer to Appendix.
4. Click **Add Network**.

If the network IP that you have entered has already been added to the database and discovered by Web NMS, relevant message is displayed in the Add Network dialog box.

## Deleting Object and Traces

Network elements that no more need to be managed can be deleted from the client as well as from the database. You can either delete a complete network or only a few elements in that network.

To delete a network

1. From the **ipnet** map or **Network Database** view, choose the network to be deleted.
2. From **Network** menu, choose **Delete Object and Traces**. A confirmation is asked.
3. Click **Yes**.

On performing this, the network as well as the elements in that network is deleted from the client as well as from the database.

To delete a device

1. From any of the sub-network maps or the Network Database view, choose the device to be deleted.
2. From **Node** menu, choose **Delete Object and Traces**. A confirmation is asked.
3. Click **Yes**.

On performing this, the device is deleted from the client as well as from the database.

## Refreshing a Node

To rediscover a node in the network, use the Refresh Node option. A node or device could have been down for a while or it would not have been discovered when you performed a manual discovery of that node. In these cases, refresh the node manually to obtain its latest information.

To refresh a node

1. In the sub-network map or Network Database view, choose the device for which you need to gather latest information by refreshing it.
2. From **View** menu, choose **Refresh**. The status of the operation is displayed in the status bar.

### 6.3.3 Configuring Discovery Filters

Web NMS constructs Managed Objects (MOs) for each of the discovered devices based on their properties. Sometimes, the properties collected for a device may not be sufficient to manage it (the device) in a network. In such cases, Web NMS provides a mechanism through which you can collect additional properties of a device and add them to the MO (before the MO is added to the topology database).

This is done using the **discovery.filters** file located in the <Web NMS Home>/conf directory. The conventional process of configuring the MO properties is by manually incorporating the user-written discovery filter classes into the **discovery.filters** configuration file and restarting the server. The **discovery.filters** file of <Web NMS Home>/conf directory incorporates the various user-defined java filter classes which define the properties of MO based on which the filtering of discovered objects of a network is accomplished.

You can configure the discovery process by simply specifying the discovery filter class name in the **Discovery Filters** in the **Runtime Administration** tool without undergoing the hassles of restarting the server.

#### To configure Discovery Filters

1. In the Web NMS Client, from **Tools** menu, choose **Runtime Administration**. The **Runtime Administration** tool is displayed.
2. From the **Categories** drop-down box or tree, choose **Topology > Discovery Filters**. The **Discovery Filter Configuration** tool is displayed on the right-side frame. All the filters that have already been configured are displayed here. The execution of these filters is based on the hierarchy in which they are placed in this tool. You can rearrange the order by dragging and dropping.
3. To **add** a new discovery filter
  - Click **Add**. The **Filter Configuration** dialog box is displayed.
  - Enter the filter class name with its package structure (if available) in **Class Name** field.
  - Click **OK**.
4. To **modify** an existing filter
  - Select the filter and click **Modify**. The **Filter Configuration** dialog box is displayed.
  - Make necessary modifications and click **OK**.
5. To **delete** a filter
  - Select the filter and click **Delete**. A confirmation is asked.
  - Click **Yes**.
6. To load the latest modified java class files into the server, i.e., updating the corresponding conf file after setting its classpath, without undergoing the hassles of manual entry into the server-side conf file, click **Reload**. To view the classpath settings, select a filter and from **File** menu, click **Classpath Settings**.
7. To save the newly added filter and modifications to the server-side **discovery.filters** file, click **Apply To Server**.

## 6.3.4 ManagedObject UI Settings

After the discovery of devices in a network, based on its properties, Web NMS constructs Managed Objects (MO) for each of the devices. For every type of MO, a related object-specific menu for accessing the characteristics of the MO through a UI is created. This configuration is specified in **listIcon.data** file located in the <Web NMS Home>/conf directory.

The **listIcon.data** file contains

- entries of all the discovered objects of Web NMS with their type
- corresponding object-specific menu
- list of image files of the respective MO (images of the MO represented for various severity colors).

The details regarding the MO are displayed in the Network Database view.

The conventional method of configuring the MO UI Settings is by editing the server-side **listIcon.data** file and restarting the server. You can also edit this file using the **ManagedObject UI Settings** in **Runtime Administration Tool** without undergoing the hassles of restarting the server.

### To configure the MO UI Settings

1. In the Web NMS Client, from **Tools** menu, choose **Runtime Administration** or press **Alt+R**. The **Runtime Administration** tool is displayed.
2. From the **Categories** drop-down box or the **Categories** tree, choose **Topology > MO UI Settings**. The **ManagedObject UI Settings** tool is displayed on the right-side frame.

The table displays all the standard and user properties specified in the **listIcon.data** file.

**Type** column displays the type of the MO. **Menu Name** column displays the menu that is associated with each type of MO of a particular type and added in the Network Database view. **Transparent Image** column displays the image filename which contains the transparent image of the corresponding MO, i.e., image of MO whose background is not painted with severity color.

3. To search for a specific MO in the list, enter the MO type in **Search for Type** field and click **Search**. This provides searching for MOs based on their type.
4. By default, details of 10 MOs are displayed in the table. To display more number of MOs, choose the required value from **Page Length** drop-down box. When there are more number of MOs, the list spans multiple screens. To navigate from one screen to the other, use the **Previous** and **Next** buttons.
5. To add a new MO property and to set its standard and user properties, click **Add**. The **ManagedObject User Interface Settings** dialog box is displayed.
  - Enter the type of the MO in **Type** field. **Example:** HP-UX
  - Enter file name of the menu that is to be associated with that MO in **Menu File Name** field.
  - To depict the MO with a transparent image (image whose background is not painted with severity color), enable **Use Transparent Image** option. Specify the image filename in **Image Name** field and click **Update**.

If you need to depict the MO with severity background, disable **Use Transparent Image** option. For each of the severities displayed, specify an image filename and click **Update**.

- Click **OK**.

6. To modify an existing MO, select the MO and click **Modify**. The **Managed Object User Interface Settings** dialog box is displayed. Make appropriate changes and click **OK**.
7. To view the details of an MO, select the MO and click **View Details**.
8. To delete an existing MO, select the MO and click **Delete**. A confirmation is asked. Click **Yes** to delete the selected MO.
9. Click **Apply**. Now the configurations made are applied to the **listIcon.data** file located in <Web NMS Home>/conf directory.

## 6.3.5 Setting User Privileges

You can restrict a user from accessing certain data in the Web NMS Client and also confine him to viewing and working on selected network topology information only. This can be achieved using the **Custom View Scope** mechanism of the Security Management. For more information, refer to Managing Custom View Scopes.

The Custom View Scope

- enables controlled view of data (only authorized data can be seen on the client)
- has improved security functions
- enables effective administration

If you have configured Custom View Scope, the changes or restrictions made can be viewed in the Network Database view.

This topic provides an example based on which you can create your own Custom View Scopes.

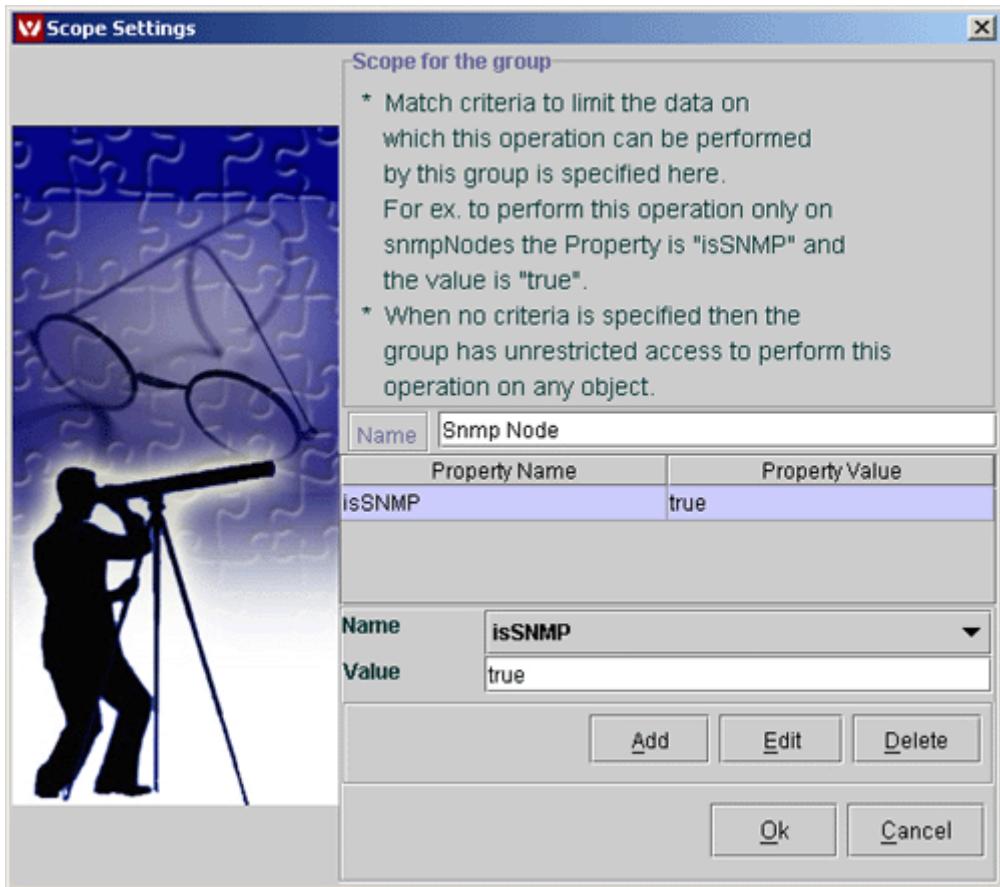
### Example

This example aims at enabling a set of users belonging to a particular group to view details pertaining to SNMP Nodes alone, on the Network Database view.

#### Procedure

1. In Web NMS Client, from **Tools** menu, choose **Security Administration**. The **Security Administration** tool is displayed.
2. Add a new user named **user1**.
3. Add a new group named **TopoGroup**.
4. Assign required permissions for the TopoGroup.
5. Assign the three new users to the TopoGroup.
6. Set the Scope Criteria.
  - Select the **TopoGroup** on the **Security** tree.
  - Click **Custom View Scope for Group** tab on the right-side frame.
  - From **Custom View Scope for Group** drop-down box, choose **Network Database**.
  - Click **Add AuthorizedScope**. The **Scope Settings** dialog box is displayed. Enter the **Name** as **Snmp Node**. From **Name** drop-down box, choose the property as **IsSNMP** and enter the **Value** as **true**. For information on each of the properties listed in the **Name** drop-down box, refer to Appendix in User Guide.
  - Click **Add**.
  - Click **OK**.

A screen shot depicting the procedure is given below.



### Result

When **user1** belonging to the group **TopoGroup** logs in, only the nodes that have the property **IsSNMP** set as true is visible on the Network Database view of the Web NMS Client.

## 6.3.6 Configurable Discovery Parameters

The discovery process can be administered by configuring the following parameters in **topodb.DBServer** process in the file **NmsProcessesBE.conf** located in the <Web NMS Home>/conf directory.



**Note:** If you have configured any of the parameters, ensure to restart the Web NMS Server.

The parameters that can be configured by administrators are listed below. For complete information, follow the links provided for each of the parameters.

- To enable the discovery and management of sub-networks -  
`MANAGE_OTHER_NETWORKS`
- To suppress the generation of info events - `SUPPRESS_INFO_EVENTS`
- To enable the status polling for sub-networks, without discovering the sub-networks -  
`DISCOVER_OTHER_NETWORKS`
- To disable the process of querying the individual nodes, which did not respond for the broadcast message - `DISCOVERY_BC_RESP_IPS`
- To disable the broadcast message, for all the IPs or nodes outside the specified range in seed.file - `STOP_BC_FOR_NETWORKS`

## 6.4 Configuring Maps

This topic explains the administrative tasks that can be performed in the Web NMS Client Maps.

---

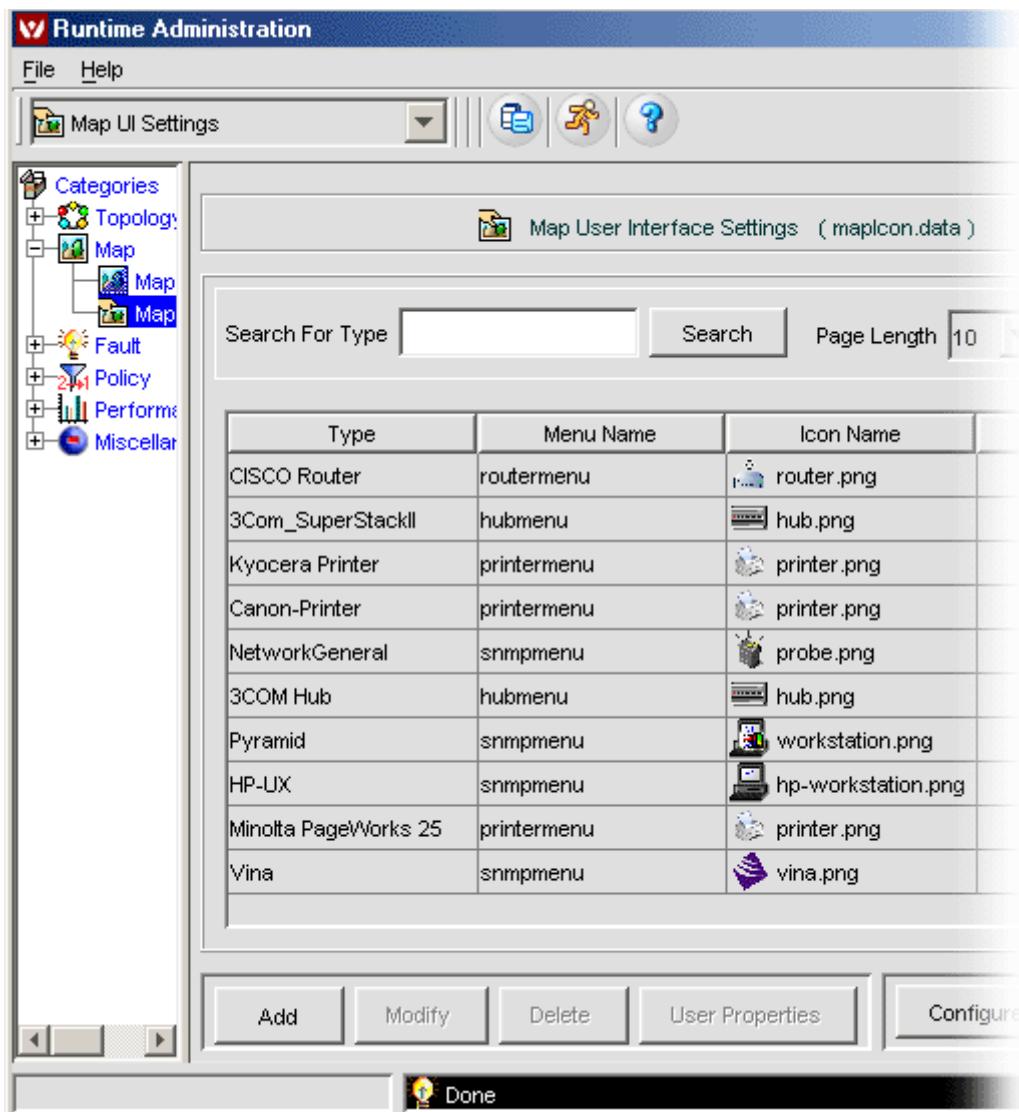
- Map UI Settings
  - Setting User Privileges
-

## 6.4.1 Map UI Settings

After the discovery of devices in a network, based on their properties, Web NMS constructs Managed Objects (MOs) for each of the devices. For every MO type, based on the information in **maps.conf** file located in the <Web NMS Home>/conf directory, a corresponding map symbol is created. You can change the properties of the map symbol by editing the **map.filters** file located in the <Web NMS Home>/conf directory.

To edit or set the map symbols corresponding to an MO that is displayed in the Web NMS Client, you need to specify the type, menu name, and the icon filename for that MO in the **mapIcon.data** file located in the <Web NMS Home>/conf directory.

The conventional method of configuring the Map UI Settings is by editing the server-side **mapIcon.data** file and restarting the server. You can also edit this file using the **Map UI Settings** in the **Runtime Administration** tool without undergoing the hassles of restarting the server.



### To configure the Map UI Settings

1. In the Web NMS Client, from **Tools** menu, choose **Runtime Administration** or press **Alt+R**. The **Runtime Administration** tool is displayed.
2. From the **Categories** drop-down box or the **Categories** tree, choose **Map > Map UI Settings**. The **Map User Interface Settings** tool is displayed on the right-side frame.

The table displays all the standard and user properties specified in the **mapIcon.data** file.

**Type** column displays the type of the MO. **Menu Name** column displays the menu that is associated with each type of MO of a particular type and added to the Network Database view. **Transparent Image** column displays the image filename which contains the transparent image of the corresponding MO, i.e., image of MO whose background is not painted with severity color. **Map Filter** is the filter class defined for a particular type of MO which creates map as per the description in the class when applied to server.

3. To search for a specific MO in the list, enter the MO type in **Search for Type** field and click **Search**. This provides searching MOs based on their type only.
4. By default, details of 10 MOs are displayed in the table. To display more number of MOs, choose the required value from **Page Length** drop-down box. When there are more number of MOs, the list spans multiple screens. To navigate from one screen to the other, use the **Previous** and **Next** buttons.
5. To add a new MO property and to set its standard and user properties, click **Add**. The **Map User Interface Settings** dialog box is displayed.
  - Enter the type of the MO in **Type** field. **Example:** switch
  - Enter file name of the menu that is to be associated with that MO in **Menu File Name** field.
  - Specify the filename of the icon to be depicted for that MO.
  - Enter the map filter name.
  - Click **Next**.
  - Enter the property key and value in **Property Key** and **Property Value** fields respectively. The values of the standard properties of a Map Symbol, such as the x,y,z coordinates of the symbol, isAnchored, etc., can be manipulated by specifying the property name and value.
  - Click **Add**.
  - Click **Finish**.
6. To modify an existing MO, select the MO and click **Modify**. The **Map User Interface Settings** dialog box is displayed. Make appropriate changes and click **Finish**.
7. To view the user properties of an MO, select the MO and click **User Properties**.
8. The **objType** property of a Map Symbol can be used to identify the type of device that the map symbol represents. Depending on the value of this property, the map symbol renderer paints the symbol background and shape accordingly. There are seven object types with their integer mapping ranging from 0 to 6 (obj Type=1 is the default). Click **Configure Object Types** to configure the object type. The **Obj Type Dialog** is displayed. Enter the object type and its integer value. On applying this configuration it overrides the corresponding property specified in the **mapIcon.data** file.
9. To delete an existing MO, select the MO and click **Delete**. A confirmation is asked. Click **Yes** to delete the selected MO.
10. Click **Apply**. Now the configurations made are applied to the **mapIcon.data** file located in **<Web NMS Home>/conf** directory.

## 6.4.2 Setting User Privileges

You can restrict a user from accessing certain data in the Web NMS Client and also confine him to viewing and working on selected network map information only. This can be achieved using the **Custom View Scope** mechanism of the Security Management. For more information, refer to Managing Custom View Scopes.

This topic provides an example based on which you can create your own Custom View Scopes for Maps.

### Example

Assume that there are three users, namely **User A**, **User B**, and **User C**. This example aims at enabling these users belonging to particular groups to view information of selected devices only.

User Name	Belongs to	Authorized Operations of the Group	Scope Criteria for the Authorized Scope of the Group	Description about the Map View of the User and the Authorized Operations
User A	Group A	Map Editing Operations	parentNet=192.168.4.0	<p>Symbols representing device which belong to 192.168.4.0 network alone will be displayed in the map of User A or any user who belongs to this group.</p> <p>User will be able to do all operations in maps.</p>
User B	Group B	Map Editing Operations	parentNet=192.168.4.0 type=win*	<p>Symbols representing devices belonging to 192.168.4.0 network and whose <i>type</i> is <b>windows</b> alone will be displayed in the map client of User B or any user who belongs to this group.</p> <p>User will be able to do all operations on maps.</p>
User C	Group C	-	parentNet=192.168.4.0 type=linux	<p>Symbols representing devices belonging to 192.168.4.0 network and whose <i>type</i> is <b>linux</b> alone will be displayed in the map client of User C or any user who belongs to this group.</p> <p>User cannot do any operations on maps as the map editing operations are not allowed for them. (or to any user in Group C)</p>



**Note:** Under situations such as the one stated in this example where many users view the same map information in the same map, there is a possibility of overlapping of symbols when one user repositions the symbols and saves the map. Hence, it is advised that the administrators provide the **save** permission for selected users alone.

To achieve this, follow the procedure given below.

## Procedure

1. In Web NMS Client, from **Tools** menu, choose **Security Administration**. The **Security Administration** tool is displayed.
2. Add new user **User A**, **User B**, and **User C**.
3. Add new groups **Group A**, **Group B**, and **Group C**.
4. Assign required permissions to the Groups.
5. Assign the 3 new users **User A**, **User B**, and **User C** to **Group A**, **Group B**, and **Group C** respectively.
6. Set the Scope Criteria.
  - Select the **Group A** on the **Security** tree.
  - Click **Custom View Scope for Group** tab on the right-side frame.
  - From **Custom View Scope for Group** drop-down box, choose **Maps**.
  - Click **Add AuthorizedScope**. The **Scope Settings** dialog box is displayed. Enter the **Name** as **Scope A**. From **Name** drop-down box, select the property as **parentNet** and enter the **Value** as **192.168.4.0**.
  - Click **OK**.
  - Perform the same steps to create custom view scopes for **Group B** and **Group C**.

On executing this example, log in to the Web NMS Client using the 3 newly added user names. The screen shots of maps as viewed by the 3 users are given below.

### Map View of User A

The map view of User A (or any user who is a part of Group A) displays all the devices in the 192.168.4.0 network.

### Map View of User B

The map view of User B (or any user who is a part of Group B) displays all the Windows devices in the 192.168.4.0 network.

### Map View of User C

The map view of User C (or any user who is a part of Group C) displays all Linux devices in the 192.168.4.0 network.

## 6.5 Fault Management

The detection of fault is an online process that gives indication of malfunctioning. Fault detection and notification are two functional areas which should identify problems and effectively inform the system administrator. Fault Management handles error conditions (that cause users to lose the full functionality of a network resource) and provides network administrators with sophisticated event management, including generation of alerts, automated actions, event correlation, trap/event/alert filtering, trap/event parsing, etc. to detect, isolate, and repair malfunctions in the network and its control sub-system.

This chapter explains

---

- Configuring Trap Port
  - Configuring Trap Parsers
  - Configuring Event Parsers
  - Configuring Event Filters
  - Configuring Alarm Filters
  - Performing Alarm Operations
  - Setting User Privileges
  - Configurable Parameters
-

## 6.5.1 Configuring Trap Ports

**Trap port** is the port at which the Web NMS Server listens for SNMP notifications. As an administrator, you can configure the trap ports from the Web NMS Client.

### To configure trap ports

1. In the Web NMS Client, click **Fault Management > Network Events** node on the tree.
2. From the **Edit** menu, choose **Configure > Trap Parsers** or press **Ctrl+Shift+R**. The **Trap Parser Configuration** dialog box is displayed.
3. Click **Modify Trap Parser**.
4. Specify the port number in the **Trap Port** field.
5. Click **Update**.
6. Click **Apply to Server**.

	<b>Note:</b> <ul style="list-style-type: none"><li>1. The specified Ports are not associated with a particular Trap Parser, but a general configuration.</li><li>2. When no port is specified, traps will not be received at all.</li><li>3. Multiple ports can be specified using a comma separator, for example - 8001,8002</li><li>4. The default configuration for Trap Port (listed in the Trap Port field) will be the port(s) specified in the &lt;Web NMS Home&gt;/conf/trapports.conf</li><li>5. Ensure that the specified ports are free.</li></ul>
---	---

## 6.5.2 Configuring Trap Parsers

Traps are cryptic messages of a fault occurred in an SNMP device. These traps must be represented in a human-readable form, and more importantly, as administrative messages that completely define the problem. Since every piece of information available in the fault report can be accessed, it is possible to define the messages exactly as required.

When a trap is received, **Trap Parsers** generate useful and appropriate event information. In the overall event flow, a received trap is passed through a level of Trap Parsers only if the trap has not been converted into an event object by a Trap Filter, or if the received trap has not been dropped during trap filtering. The output of a Trap Parser is an event object.

The Trap Parsers that are saved in the **trap.parsers** file located in the *<Web NMS Home>/conf* directory load automatically when the server is restarted and listed in the Configured Trap Parser list. The incoming traps are processed through the list of configured Trap Parsers. The order of this list can be changed.

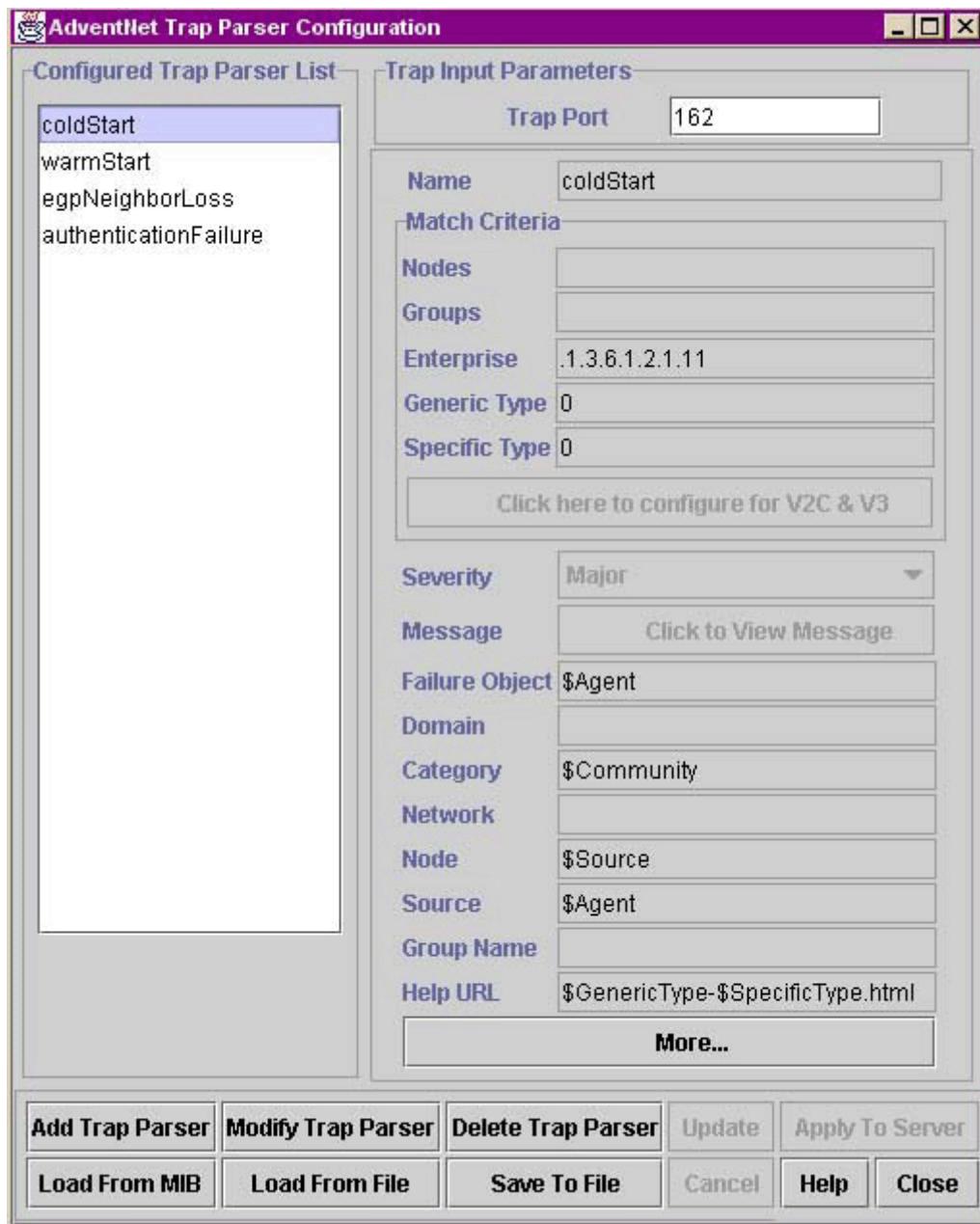
The match criteria in the parser determine whether a specific trap matches the Trap Parser. The search for matching Trap Parsers is done based on how the Trap Parsers are ordered in the list. Once a matching Trap Parser is found, an event is generated by applying the corresponding Trap Parser. Only one Trap Parser is applied to a given trap and no other Trap Parsers are applied to that trap.

You can complete the following procedures when configuring Trap parsers:

- 
- Opening the Trap Parser Configuration Tool
  - Adding Trap Parsers
  - Loading Trap Parsers from a MIB
  - Modifying Trap Parsers
  - Saving Trap Parser Files
  - Loading Trap Parser Files
  - Reordering the Configured Trap Parser List
  - Enabling and Disabling Trap Parsers
  - Deleting Trap Parsers
-

## Opening the Trap Parser Configuration Tool

The Trap Parsers can be created or modified using the **Trap Parser Configuration** tool.



### To open the Trap Parser Configuration Tool

- In the Web NMS Client, click **Fault Management > Network Events** node on the tree. From **Edit** menu, choose **Configure > Trap Parsers** or press **Ctrl+Shift+R**. The **Trap Parser Configuration** dialog box is displayed.

Or

- In the Web NMS Launcher, from **Administrator Tools**, invoke **Trap Parser**.

Or

- Execute the script file **TrapParserConfig** located in the <Web NMS Home>/bin/admintools directory.

	<p><b>Note:</b> The <b>Trap Parser Configuration</b> tool invoked from launcher or using script is an offline configuration tool.</p> <ul style="list-style-type: none"> <li>• Hence it does not have the <b>Add To Server</b> option.</li> <li>• While loading Trap Parsers from a MIB, specify the MIB path relative to &lt;Web NMS Home&gt; directory.</li> </ul>
---	--

## Adding Trap Parsers

### To add a Trap Parser

1. In the **Trap Parser Configuration** dialog box, click **Add Trap Parser**. All the fields in the dialog box are enabled.
2. Enter values for the **Trap Input Parameters**. For information on each of the fields, refer to Configuring Trap Parsers section in Appendix.

While specifying the output values for the event object that is generated in the fields, you can use information in the incoming trap Protocol Data Unit (PDU) information. The information in the trap PDU can be accessed using the specifically designed tokens that represent the values of the various fields present in the trap. For information on the token values, refer to Trap Protocol Data Unit Information section in Appendix.

3. To specify your own properties to the event object generated by the Trap Parser, click **More**. The **Trap Parser Configuration** dialog box is displayed.

Enter the name and the value of the property in **Property Name** and **Match Criteria** fields respectively. To enter more properties, click **More**. When you are finished adding values and properties, click **OK**.

4. Click **Update**. The newly configured Trap Parser is added to the **Configured Trap Parser List**.
5. To apply this configuration to the server, click **Apply To Server**.

## Viewing Trap Parser Details

### To view details of a Trap Parser

1. From the **Trap Parser Configuration** dialog box, click the Trap Parser you want to view in the **Configured Trap Parsers List**.
2. The Trap Parser details are listed in the fields.
3. When you are finished viewing the parser details, click **Close**.

## Loading Trap Parsers from a MIB

Instead of manually creating a Trap Parser, you can load defined traps from a Management Information Base (MIB). These traps can be translated into Trap Parsers.

### To load Trap Parsers from a MIB

1. From the **Trap Parser Configuration** dialog box, click **Load From MIB**. The **Load Trap Parsers From MIB** dialog box is displayed.

2. Enter the filename of the MIB in the **Load MIB Filename** field.

The filename should include the path relative to the <Web NMS Home>/mibs directory. If the MIB depends on any other MIB files, specify those dependency files with spaces in between them followed by the MIB file you want to load.

**Example:** If **A-MIB** imports **B- MIB**, which imports **C-MIB** (all the files located in <Web NMS Home>/mibs directory), specify the filename as: `../mibs/C-MIB ../mibs/B-MIB ../mibs/A-MIB`

However, the Trap Parsers are created from the last MIB file only.

3. Click **Create Parsers**. The MIBs are loaded and Trap Parsers are created from the specified file.
4. After the Trap Parsers are created, you can set the severities and enter information in other event fields (such as, the Failure Object field) for each of the created Parsers. If the severities are not specified, the default severity (Info) is used.
5. To apply this configuration to the server, click **Apply To Server**.

## Modifying Trap Parsers

### To modify a Trap Parser

1. From the **Trap Parser Configuration** dialog box, select the Trap Parser from the **Configured Trap Parser List**.
2. Click **Modify Trap Parser**. The fields are editable. For more information on each of the fields, refer to Configuring Trap Parsers section in Appendix.

While specifying the output values for the event object that is generated in the fields, you can use information in the incoming trap Protocol Data Unit (PDU) information. The information in the trap PDU can be accessed using the specifically designed tokens that represent the values of the various fields present in the trap. For information on the token values, refer to Trap Protocol Data Unit Information section in Appendix.

3. To specify your own properties to the event object generated by the Trap Parser, click **More**.

The **Trap Parser Configuration** dialog box is displayed.

Enter the name and the value of the property in **Property Name** and **Match Criteria** fields respectively. To enter more properties, click **More**. When you are finished adding values and properties, click **OK**.

4. Click **Update**. The newly configured Trap Parser is added to the **Configured Trap Parser List**.
5. To apply this configuration to the server, click **Apply To Server**.

## Saving Trap Parser Files

To reuse or to retain the configured Trap Parsers, ensure to save the Trap Parser file. By default, all the Trap Parsers and their configurations are saved in **trap.parsers** file located in the <Web NMS>/conf directory.

### To save a Trap Parser file

1. From the **Trap Parser Configuration** dialog box, click **Save To File**. The **Save Trap Parsers To File** dialog box is displayed.
2. By default, the filename is **trap.parsers**. If you do not want to overwrite this file, enter a new filename in **Filename** field.
3. Click **Save**.

## Loading Trap Parser Files

Previously saved Trap Parsers can be loaded to the **Trap Parser Configuration** tool.

### To load a Trap Parser File

1. From the **Trap Parser Configuration** dialog box, click **Load From File**. The **Load Trap Parsers From File** dialog box is displayed.
2. Enter the filename in **Filename** field.
3. Click **Load**. The Trap Parsers from the specified file are loaded. **Note:** Any Parsers with the same match criteria as that of the existing ones currently listed in the **Configured Trap Parser List** are replaced with the Trap Parsers from the loaded file.

## Reordering the Configured Trap Parser List

The incoming traps are processed through the list of configured Trap Parsers, and only one Trap Parser is applied to a given trap. The Trap Parsers are applied to the trap based on their order as listed in the **Configured Trap Parser List**.

### To reorder the configured Trap Parser list

1. From the **Trap Parser Configuration** dialog box, click and drag the Trap Parser you want to reorder in the **Configured Trap Parser List** to a new location in the list.
2. To save this configuration in the server, click **Apply To Server**.

## Enabling and Disabling Trap Parsers

To enable or disable a Trap Parser, you need to edit the file where you have configured the Trap Parsers. By default, the Web NMS Trap Parsers are configured in **trap.parsers** file.

### To enable/disable Trap Parsers

1. Edit the file **trap.parsers** file located in the <Web NMS Home>/conf directory.
2. Edit the **enable** parameter in the <PARSER> tag of a Trap Parser. If the **enable** value is set **true**, then the corresponding parser is enabled; and if it is set **false**, it is disabled. The default value of **enable** is set **true**.

Example:

```
<PARSER textDefn="" helpDefn="" type="0" nodeDefn="$Source"
networkDefn="" GT="1" ST="0" enable="true" name="warmStart" />
</PARSER>
```



**Note:** The enabling/disabling of Trap Parsers can be done only by editing the **trap.parsers** file and not through the **Trap Parser Configuration** tool.

## Deleting Trap Parsers

### To delete a Trap Parser

1. From the **Trap Parser Configuration** dialog box, select the Trap Parser from the **Configured Trap Parser List**.
2. Click **Delete Trap Parser**. **Tip:** You can also delete a Trap Parser by pressing the Delete key on the keyboard. Two or more Trap Parsers can be deleted by holding the Ctrl key and selecting the Trap Parsers you want to delete and then pressing the Delete key.
3. A confirmation is asked. Click **Yes** to delete the Trap Parser.
4. To save this configuration to in the server, click **Apply To Server**.

### 6.5.3 Configuring Event Parsers

To identify the failure object corresponding to an event, the traps and the input events should be parsed and the necessary details should be displayed. The Trap Parser makes the notifications readable to the user. Event Parsers refine the message conveyed by the events. Though both the Trap Parser and Event Parser seem to function identically, the Event Parser converts other types of events, such as threshold events, status poll events, into a readable format before the events are filtered.

When an event reaches the Web NMS server, the Event Parser list is checked to see whether the incoming event satisfies the match criteria of the Event Parser. If matched, the event is passed through the corresponding Event Parser. The outgoing event from the Parser is then matched with the remaining set of Parsers (if any and in sequence). If there are any matches, the event is passed through those Parsers also. This process continues until all the Parsers are scanned.

By default, the Event Parsers saved in the **event.parsers** file located in the <Web NMS Home>/conf directory are loaded automatically when the server is booted. These Parsers are displayed in the **Event Parser Configuration** dialog box.

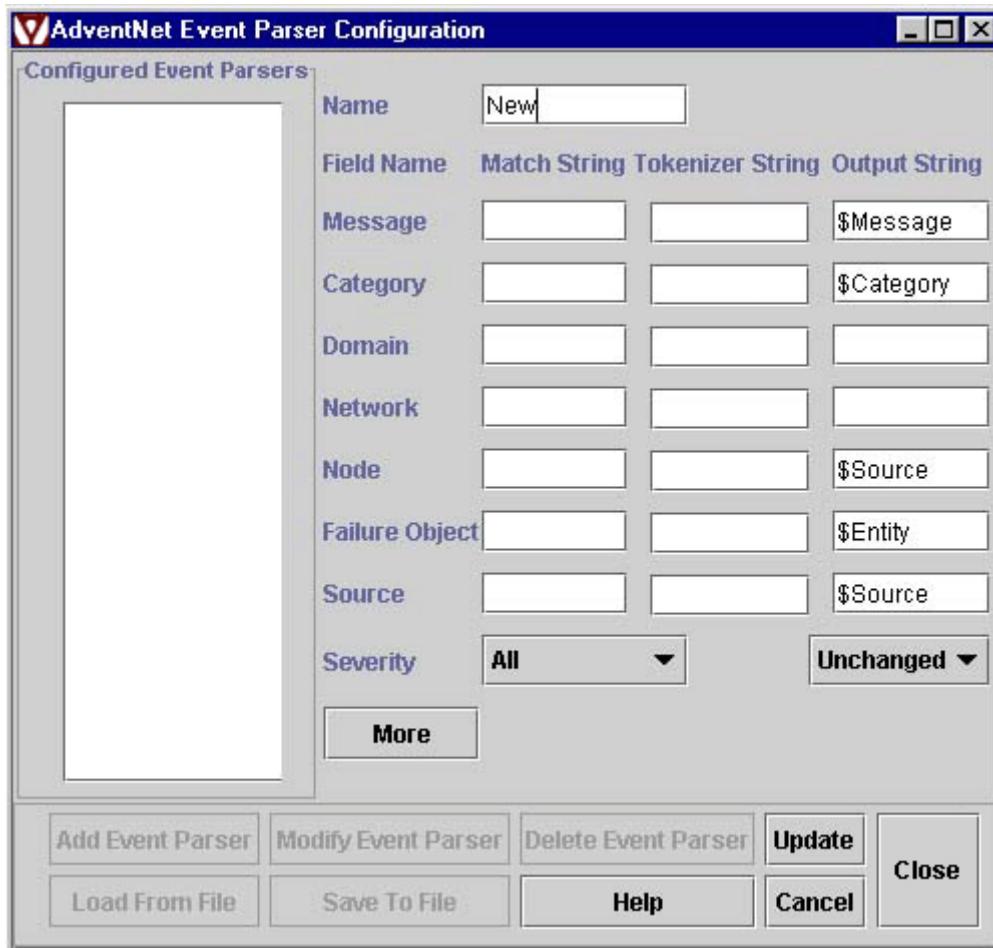
You can complete the following procedures when configuring Event Parsers:

---

- Opening the Event Parser Configuration Tool
  - Adding Event Parsers
  - Modifying Event Parsers
  - Saving Event Parser Files
  - Loading Event Parser Files
  - Reordering the Configured Event Parser List
  - Enabling and Disabling Event Parsers
  - Deleting Event Parsers
-

## Opening the Event Parser Configuration Tool

The Event Parsers can be created or modified using the **Event Parser Configuration** tool.



### To open the Event Parser Configuration Tool

- In the Web NMS Client, click **Fault Management > Network Events** node on the tree. From **Edit** menu, choose **Configure > Event Parsers** or press **Ctrl+E**. Or
- In the Web NMS Launcher, from **Administrator Tools**, invoke **Event Parser**. Or
- Execute the script file **EventParserConfig** located in the <Web NMS Home>/bin/admintools directory.

The **Event Parser Configuration** dialog box is displayed.

	<b>Note:</b> The <b>Event Parser Configuration</b> tool invoked from launcher or using script is an off-line configuration tool. Hence it does not have the <b>Add To Server</b> option.
--	--

## Adding Event Parsers

### To add an Event Parser

1. In the **Event Parser Configuration** dialog box, click **Add Event Parser**. All the fields in the dialog box are enabled.
2. Specify a name for the Event Parser for distinct identification in the **Name** field.
3. Further, specify appropriate values in the fields (tabulated below). The values for each of these fields can be specified as **Match String**, **Tokenizer String**, or **Output String**. Explanation on these is provided below the table.

Field	Description
Message	Corresponds to the text field of the event object.
Category	Categorizes events and alarms.
Domain	Domain name of an event.
Network	Identifies the network name from which the event has originated.
Node	Node value of an event.
Failure Object	Tracks problems and identifies objects.
Source	Identifies the source name of an event.
Severity	Indicates the state of an event.

**Match String:** The match criteria in the Event Parser Configuration dialog box determine whether the event will be parsed by the given event parser. If a field is left blank, it is automatically matched; otherwise, all fields (AND condition applied) must match the input event. To specify the match criteria, the following may be used in expressions:

- **Wild Card Character - Asterisk ( \* ):** Signifies match 0 or more characters of any value. For example, \*Failed\* matches any string containing Failed.
- **Negation - Exclamation ( ! ):** Used at the start of a field to specify exclusion of events matching the succeeding expression. For example, !Failed excludes strings containing Failed.

**Note:** Expressions, such as \*Failed, Fai\*d, and \* have the expected meanings in the match criteria.

**Tokenizer String:** Enables you to separate the input field into a series of tokens that can be used in the output event object. The tokenizer definition is a string with tokens represented by \$1, \$2, etc. Only positive integers are allowed following the dollar sign (\$).

### Example

Consider the case, where you expect an event message text string, such as

Line Card 31 failed on Shelf 54: No Response – Match String

Using the Line Card Number (31), the Shelf Number may be required when defining other properties of the event. You need to tag these properties as tokens with a token number:

Line Card \$1 failed on Shelf \$2: No Response – Tokenizer String

After such tokenization, you can use the token number in the output event definition.

Specifying **\$text\$1** for any field in the output event definition, replaces the string with the value 31; similarly specifying **\$text\$2**, replaces the string with 54.

	<b>Note:</b> <ol style="list-style-type: none"> <li>1. To identify the replaceable parameter of a specific field, the token number should be preceded by the field. For example, <b>\$text\$1</b> indicates the first tokenized string of the field Message.</li> <li>2. The tokens of any field can be used in any other field provided that paragraph (1) is followed.</li> </ol>
---	---

**Output String:** The output string of the event parser is an event object that becomes the modified instance of the incoming event. The attributes of the event object are defined by the specifications in the event parser. It is necessary to select correct values, particularly for important attributes, namely failure object (affected entity), severity, and message text.

The properties that should remain unchanged must be specifically noted by placing a dollar sign followed by the property name. For example, if the text field should not be modified, then the value **\$text** should be entered in the output string.

To use the values of the incoming event properties while specifying the output values in the definition column, specify the exact property name (case sensitive) with a prefixed **\$**. For example, to use the event property **Source**, the definition should be **\$source**. If the particular property has been tokenized and if you intend to use the value of the token, then the format should be **\$propertyname\$N**, where N is the count of the token starting with 1.

When it is necessary to deliberately have a null value for a specific property of the output event, the output string for that property should be left blank.

The default properties of an event that can be used in the definition column following the dollar sign (\$) are, category, domain, entity, groupName, helpURL, network, node, source, severity, and text.

While specifying the output values for the event object that is generated in the fields, you can use information in the incoming trap Protocol Data Unit (PDU) information. The information in the trap PDU can be accessed using the specifically designed tokens that represent the values of the various fields present in the trap.

	<p><b>Important:</b> The methodology of using the properties of the trap using symbolic notations is similar to that of Trap Parsers, except for the following difference.</p> <ul style="list-style-type: none"> <li>• To access the values of the SNMP OID in the SNMP Variable bindings, the notation should start with <b>%</b> and not with <b>\$</b> as in trap parser.</li> <li>• All the special purpose tags should start with <b>%</b> instead of <b>\$</b> as in trap parser.</li> <li>• To access the SNMP OID in the SNMP Variable bindings, the notation should start with <b>@</b> which is same as in Trap Parser.</li> </ul> <p>The values of the trap PDU can be used in any of the columns, except in Tokenizer, in the Parser defined. For information on the token values, refer to Event Properties section in Appendix. The trap PDUs explanation is the same for Trap Parsers, Event Parsers, and Event Filters (only % and \$ notations differ). For information on PDU, refer to Trap Protocol Data Unit Information section in Appendix.</p>
---	---

## Example

Field	Match String	Tokenizer String	Output String	Value
Message	<i>Line Card 31 failed on Shelf 54: No Response</i>	<i>Line Card \$1 failed on Shelf \$2: No Response</i>	Failure occurred on \$source\$1 Shelf \$text\$2 LineCard \$text\$1	Failure occurred on SwitchA Shelf 54 LineCard 31
Source	SwitchA	\$1	-	-

5. To specify your own properties to the event object generated by the Event parser, click **More**. The **Event Parser Configuration** dialog box is displayed.

Specify the name and the value of the property in **Property Name** and **Match Criteria** fields respectively. To enter more properties, click **More**. When you are finished adding values and properties, click **OK**. For information on properties, refer to Event Properties in User Guide > Appendix.

**Note:** If a criterion is configured based on the Event user property and if no definition is given against that property, then the user property is dropped in the resulting Event. The event properties **id** and **time** are not configurable using the event parsers. These fields will be copied to the values as that of the incoming event object.

6. Click **Update**. The newly configured Event Parser is added to the **Configured Event Parser List**.
7. To apply this configuration to the server, click **Apply**.

## Modifying Event Parsers

### To modify an Event Parser

1. In the **Event Parser Configuration** dialog box, select the Event Parser to be modified, from **Configured Event Parsers**.
2. Click **Modify Event Parser**. All the fields in the dialog box are enabled.
3. To specify your own properties to the event object generated by the Event Parser, click **More**. The **Event Parser Configuration** dialog box is displayed.

Specify the name and the value of the property in **Property Name** and **Match Criteria** fields respectively. To specify more properties, click **More**. When you are finished adding values and properties, click **OK**.

4. Make appropriate changes and click **Update**.
5. To apply this configuration to the server, click **Apply**.

## Saving Event Parser Files

### To save Event Parser files

1. In the **Event Parser Configuration** dialog box, click **Save To File**. The **Save Event Parsers To File** dialog box is displayed.

2. By default, the configurations are saved in **event.parsers** file located in the <Web NMS Home>/conf directory. Specify a different filename, if required. The relative base directory for saving these files is <Web NMS Home>.
3. Click **Save**.

## Loading Event Parser Files

Previously saved Event Parsers can be loaded to the existing parsers list.

### To load an Event Parser file

1. In the **Event Parser Configuration** dialog box, click **Load From File**. The **Load Event Parsers From File** dialog box is displayed.
2. Specify the filename.
3. Click **Load**.

**Note:** Any Parsers with the same match criteria as that of the existing ones currently listed in the Configured Event Parser list are replaced with the Event Parsers from the file that you load.

## Reordering the Configured Event Parser List

Since incoming traps are processed through the list of configured Event Parsers, and only one Event Parser is applied to a given trap, the order of this list can be changed.

### To reorder Event Parser list

- In the **Event Parser Configuration** dialog box, click and drag the Event Parser you want to reorder in the **Configured Event Parser** list to a new location in the list.

## Enabling and Disabling Event Parsers

The configured Event Parsers can be enabled or disabled using the parameter **enable** in the **event.parsers** file located in the <Web NMS Home>/conf directory.

```
<EVENT_PARERS>
<PARSER name="Test parser" severityDefn="Unchanged"
nodeMatch="$Source" enable="true" />
</EVENT_PARERS>
```

If the **enable** value is set **true** (default value), the corresponding Parser is enabled; and if it is set **false**, it is disabled.

**Note:** The enabling/disabling of Event Parsers can be done only by editing the **event.parsers** file and not through the **Event Parser Configuration** tool.

## Deleting Event Parsers

### To delete an Event Parser

1. In the **Event Parser Configuration** dialog box, select the Event Parser to be deleted from the **Configured Event Parsers** list.
2. Click **Delete Event Parser**. A confirmation is asked.
3. Click **Yes** to delete the Event Parser.

## 6.5.4 Configuring Event Filters

When events are generated from devices in a network, you can configure Web NMS to perform certain actions on such occurrences. For this purpose, **Event Filters** can be used which provide you a way to configure Web NMS to automatically initiate actions for select Events.

Web NMS supports the following types of built-in filter actions:

- Suppressing multiple events in a given interval
- Running shell commands on the server system
- Sending e-mails
- Sending traps
- Running custom code to filter events (custom code might be needed in cases where additional data needs to be retrieved, or if specific rules are to be applied when processing an event.)

The processed events are stored in a database and can be viewed in the Events Viewer. The Events Viewer is asynchronously notified as soon as an event is processed.

You can configure an Event Filter using the **Event Filter Configuration** tool. You can use the properties of the event object or of the associated trap (if the event has been generated by a trap) in some of the fields, such as to Suppress Action, Run Command Action, Send Trap Action, and Send E-mail Action.

**Note:** In cases where the event has been generated by a trap, the PDU information of the associated trap that generated the event can be used as tokens. For more information, see Trap Protocol Data Unit Information in Appendix.

A custom filter can be configured to enable more effective event correlation and fault management by adding application-specific rules when processing events and alarms. However, this should be done by a developer and not by an administrator.

You can complete the following procedures when configuring Event Filters:

- 
- Opening the Event Filter Configuration Tool
  - Adding Event Filters
  - Action Types
    - Suppress Action
    - Configuring Run Command Action
    - Send Trap Action
    - Send E-mail Action
    - Custom Filter
  - Modifying Event Filters
  - Saving Event Filter Files
  - Loading Event Filter Files
  - Reordering the Configured Event Filter List
  - Enabling and Disabling Event Filters
  - Deleting Event Filters
-

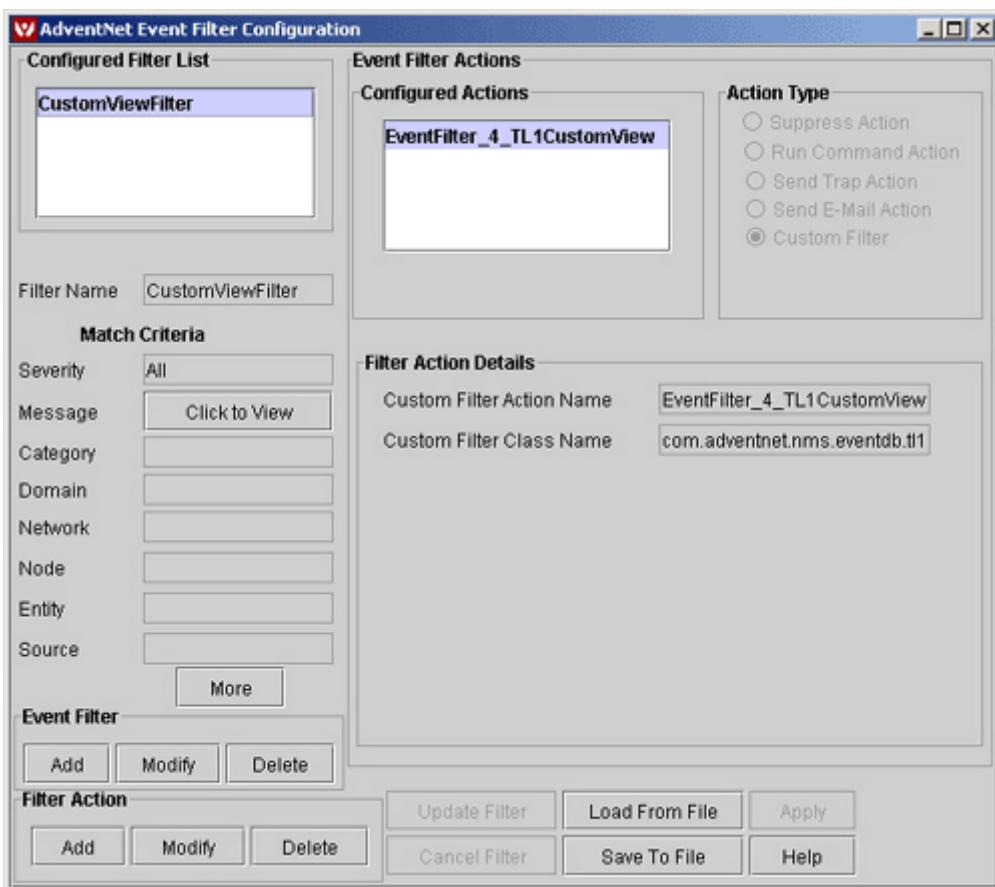
## Opening the Event Filter Configuration Tool

The Event Filters can be created or modified using the Event Filter Configuration tool.

### To open the Event Filter Configuration Tool

- In the Web NMS Client, click **Fault Management > Network Events** node on the tree. From **Edit** menu, choose **Configure > Event Filters** or press **Ctrl+Shift+E**. Or
- In the Web NMS Launcher, from **Administrator Tools**, invoke **Event Filter**. Or
- Execute the script file **EventFilterConfig** located in the <Web NMS Home>/bin/admintools directory.

The **Event Filter Configuration** tool is displayed.



**Note:** The **Event Filter Configuration** tool invoked from launcher or using script is an offline configuration tool. Hence it does not have the **Add To Server** option.

## Adding Event Filters

### To add an Event Filter

1. From the **Event Filter Configuration** tool, click **Add**.
2. Specify a name for the Event Filter in **Filter Name** field.
3. Specify appropriate values as **Match Criteria**. For information on each of the Match Criteria fields, refer to the following table.

Field	Description
Severity	Match criteria based on the severity of the event, such as Critical, Major, and so on.
Message	Match criteria based on a message of the incoming event, such as Interface failure, Status Poll failed, and so on.
Category	Match criteria based on an event object property with a category name to which the event belongs. This is used to organize events.
Domain	Match criteria based on an event object property with any domain-specific information. The information might be based upon the physical location, or the functional or logical categorization of the source of the event. The domain name of the event displays events of a particular domain.
Network	Match criteria based on the information about the network to which the source of the event belongs. Using this criteria, events belonging to a particular network are displayed.
Node	Match criteria based on any additional information (name of the node) about the source of the event.
Entity	Match criteria based on the information about an exact device in which a problem has occurred.
Source	Match criteria based on the information about the source of the event so that the events matching a source can be filtered out.

The values that you specify in the Match Criteria determine whether the incoming event should be filtered or not. If this field is left blank, it is automatically matched. For the Event Filter to be applied, all the match criteria specified must be satisfied. If even one criterion fails, the Filter will not be applied. The following expressions can be used while specifying the match criteria:

- **Wildcard - Asterisk (\*)** Use to signify a match of 0 or more characters of any value. **Example:** Failed\* matches any string starting with *Failed*. Expressions, such as \*, \*Failed, Fai\*led\*, can be used.
- **Negation - Exclamation (!)** Used at the start of the field to specify exclusion of events matching this expression. **Example:** !Failed excludes strings starting with *Failed*.
- **Separator - Comma (,)** Used to specify multiple values for a single match criterion by separating them with commas. **Example:** Critical, Major will match a string which is either *Critical* or *Major*.

The following combinations can be used while specifying match criteria.

- **\* AND , :** This combination can be used to obtain the combined result of two matching criteria that signifies a match of 0 or more characters for the given criteria. **Example:** (\*x, \*y) is tokenized into \*x and \*y and only data ending with x and y is matched.
- **! AND , :** This combination can be used to obtain the exclusion of events matching two criteria. **Example:** (!x,!y) is considered an AND operation. Hence all data starting with (x,y) is not be matched.
- **a,b :** This combination is tokenized into two strings ('a' and 'b'). Therefore this criterion matches 'a,b' and also the data 'a' and 'b'.

To specify additional match criteria for the Event Filter, click **More** and complete the following steps.

- On clicking **More**, the **Event Filter Configuration** dialog box is displayed.
- Specify the **Property Name** and **Match Criteria**. The match criteria specified must be based on the properties of **com.adventnet.nms.eventdb.Event** object including **Userproperties**. While specifying additional criteria, specify only those properties that are in the event object. The name should exactly match the case of the event object. You can also add event base properties as match criteria, such as **group name**, **help URL**, **ID**, and **time**. For more information on event properties, refer to Event Properties in User Guide > Appendix.
- To add more properties, click **More**.
- When you are finished adding properties and values, click **OK**.

4. To include a filter action whenever the incoming event satisfies the match criteria, complete the following steps:
  - In the **Filter Actions** section, click **Add**. The **Action Type** fields are enabled.
  - Choose one of the actions from **Action Type** section. For information on each of the actions, follow the links given below.
    - Suppress Action
    - Run Command Action
    - Send Trap Action
    - Send E-Mail Action
    - Custom Filter

**Note:** An Event Filter must have at least one action associated with it.

- Specify values for the selected action.
- Click **Update Action** to add the action to the configured actions list. The Update Action button toggles to the Update Filter button.
- To add more actions, click **Add** and specify values for the selected action. At any time, to abort the adding of Filter or Action, click **Cancel Filter** and **Cancel Action** respectively.

5. When you are finished adding Filter and actions, click **Update Filter**.
6. To save the configuration to the server, click **Apply**.

## Action Types

This section explains the various action types that you can configure for an Event Filter.

### Suppress Action

This Filter action allows you to suppress or drop events that match the filter criteria, either altogether or multiple events of the same type within a given interval.

For information on selecting an action type, refer to the previous section Adding Event Filters. The following are the fields that are to be configured for Suppress Action.

Field	Description
Suppress Action Name	Specify a name for the Filter action.
Suppress All	Indicates whether to suppress incoming events. <ul style="list-style-type: none"> <li>• <b>Yes:</b> Suppresses all subsequent incoming events.</li> <li>• <b>No:</b> Suppresses subsequent events during the specified interval.</li> </ul>
Suppress Interval	Specify a numeric value (in seconds) to suppress multiple events for a given interval. The first event that matches the configured criteria is allowed and all the subsequent events are suppressed for the given interval. After the suppress interval has elapsed, another event matching the criteria is allowed and the subsequent events are again suppressed, and so on.  The input for this field can be extracted from the event properties by using the replaceable parameter <b>\$&lt;Event Property&gt;</b> or from the PDU information contained in the event when the event has been generated from a trap. But in either case, it is imperative to ensure that the value returns a numeric value. For information on PDU, refer to Trap Protocol Data Unit Information section in Appendix.

## Run Command Action

This Filter actions allows you to run a command on the server for events matching particular filter criteria. It can be used to send a page to someone, e-mail, or any other desired command.

For information on selecting an action type, refer to the previous section Adding Event Filters. The following are the fields that are to be configured for Run Command Action.

Field	Description
Run Command Action Name	Specify a name for the Filter action.
Run Command	Specify the command string to be executed.  The command string should be a machine-executable program on the server that does not require a shell (it cannot be a batch or shell file).  <b>Example:</b> <i>dir</i> - Executing this command lists all the directories under <Web NMS Home> in the message field of the Event.
Command Results	To append output or errors from the command to the event message text, check one or both of the check boxes - <b>Append to Output</b> and/or <b>Append to Errors</b> .  Checking either or both check boxes results in the command being run synchronously in the main event processing thread. This delays all events that follow the event being processed until the command execution is completed or terminated by the timeout.

Abort After	Specify the time after which the command execution is to be stopped. This field is used to specify the timeout for the command. It is important if you are appending the output or errors since the entire event processing is held up by the command execution.
-------------	--

To use shell scripts or commands, you must invoke the shell as a part of the command string. The command string must contain the full path of the shell where the Event server has started.

The fields for which the tokens can be used are the command argument fields and the timeout (Abort After) field of the action. If the tokens are used for the timeout field, ensure that the dynamically generated value is numeric.

## Send Trap Action

This filter action allows you to send SNMP v1/v2c traps for events matching particular filter criteria. The traps can be configured to have event data as specified by you. It can be configured to be sent to any desired host.

For information on selecting an action type, refer to the previous section Adding Event Filters. The following are the fields that are to be configured for Send Trap Action.

Field	Description
V1 / V2C	Select the type of SNMP trap to be sent.
Send Trap Action Name	Specify a name for the Filter action.
Trap Destination	Specify the host to which the trap is to be sent.
Destination Port	Specify the port to which the trap is to be sent.
Trap Community	Specify the string to be set for the generated trap.
Enterprise	Specify the OID of the trap. Applicable only to SNMP v1.
Generic Type	Specify the number to be used for the trap. Applicable only to SNMP v1.
Specific Type	Specify the number to be used for the trap. Applicable only to SNMP v1.
SysUpTime (secs)	Specify the sysuptime value to be used in the trap.
Trap OID*	Specify the OID of the trap that is being sent. Applicable only to SNMP v2c.
Variable Bindings	<p>Click <b>Add</b> in <b>Filter Action Details</b> section to add Variable Bindings to the trap.</p> <p><b>OID Value:</b> Specify the value of the Object ID.  <b>SNMP Type:</b> Choose the appropriate SNMP string from the drop-down list.  <b>Set Value:</b> Specify the set value associated with the selected SNMP type.  Click <b>Update</b>.</p> <p>To add more Variable Bindings, click <b>Add</b> and specify the values.</p>

## Send E-mail Action

This filter action allows you to send an e-mail for events matching particular filter criteria.

For information on selecting an action type, refer to the previous section Adding Event Filters. The following are the fields that are to be configured for Send E-mail Action.

For all the Send E-mail Action fields (except Recipient's Address and Sender's Address fields), you can specify the value using the event object attributes (and associated trap, if any) using tokens

Field	Description
Send E-mail Action Name	Specify a name for the Filter action.
User Name	Specify the user name using which the mail server will authenticate you to send the email.
Password	Specify the password using which the mail server will authenticate you to send the email.
SMTP Server	Specify the SMTP server address. <b>Example:</b> example.com or 192.168.1.139
Recipient's Address	Specify the destination address to which the e-mail should be sent. <b>Example:</b> fault@example.com
Sender's Address	Specify the sender's address from which the e-mail is being sent. <b>Example:</b> john@example.com
Subject	Specify a subject of the mail.
Message	Specify the message to be sent as an email.
File Attachment	Files such as log files can be attached with the mail which will help the administrator in debugging the fault.

	<p><b>Making use of the associated trap properties in an event filter, if the event has been generated by a trap</b></p> <p>When an event is generated by a trap, the associated Trap PDU reference is maintained in the incoming event object, if the parameter <b>TRANSIENT_TRAP_PDU_IN_EVENT</b> under the <b>EventMgr</b> module in <b>NmsProcessesBE.conf</b> file located in the <code>&lt;Web NMS Home&gt;/conf</code> directory is set <b>true</b>. If the incoming event object has maintained the trap PDU reference, then you can use the properties of the trap, within the configured event filter. The properties of the trap could be used at the level of specifying match criteria (using <b>More</b> option) and also for specifying values of the various action fields. The methodology of using the properties of the trap, using symbolic notations is similar to that of Trap Parsers, except for the following differences:</p> <ul style="list-style-type: none"> <li>• To access the values of the SNMP OID in the SNMP Variable bindings, the notation should start with % and not with \$ as in trap parser.</li> <li>• All the special purpose tags should start with % instead and not with \$ as in trap parser.</li> <li>• To access the SNMP OID in the SNMP Variable bindings, the notation should start with the same @ as in trap parser.</li> </ul> <p>For more information, refer to Appendix.</p>
---	--

## Custom Filter

You can write your own Java code to filter events and perform actions, and configure them to be applied for events matching particular filter criteria. This is more of an option for the developer than an administrator.

For information on selecting an action type, refer to the previous section Adding Event Filters. The following are the fields that are to be configured for Custom Filter Action.

Field	Description
Custom Filter Action Name	Specify a name for the Filter action.
Custom Filter Class Name	Specify the custom filter's class name.

## Modifying Event Filters

### To modify Match Criteria of an Event Filter

1. In the **Event Filter Configuration** dialog box, select the Event Filter to be modified, from **Configured Filter List**.
2. Click **Modify** in **Event Filter** section. All the fields in the **Match Criteria** section are enabled.
3. To specify your own properties to the event object generated by the Event Filter, click **More**. The **Event Filter Configuration** dialog box is displayed.

Specify the name and value of the property in **Property Name** and **Match Criteria** fields respectively. To specify more properties, click **More**. When you are finished adding values and properties, click **OK**.

4. Make appropriate changes and click **Update Filter**.
5. To apply this configuration to the server, click **Apply**.

### To modify Match Criteria of an Event Filter

1. In the **Event Filter Configuration** dialog box, select the Event Filter to be modified, from **Configured Filter List**. Its corresponding actions are listed in **Configured Actions** section.
2. Select the action.
3. Click **Modify** in **Filter Action** section. All the fields in the **Filter Action Details** section are enabled.
4. Make appropriate changes and click **Update Action**.
5. To apply this configuration to the server, click **Apply**.

## Saving Event Filter Files

### To save Event Filter files

1. In the **Event Filter Configuration** dialog box, click **Save To File**. The **Save Event Filter To File** dialog box is displayed.

2. By default, the configurations are saved in **event.filters** file located in the <Web NMS Home>/conf directory. Specify a different filename, if required. The relative base directory for saving these files is the <Web NMS Home>.
3. Click **Save**.

## Loading Event Filter Files

Previously saved Event Filters can be loaded to the existing Filter list.

### To load an Event Filter file

1. In the **Event Filter Configuration** dialog box, click **Load From File**. The **Load Event Filter From File** dialog box is displayed.
2. Specify the filename.
3. Click **Load**.

**Note:** Any Filters with the same match criteria as that of the existing ones currently listed in the Configured Event Filter list are replaced with the Event Filters from the file that you load.

## Reordering the Configured Event Filter List

### To reorder Event Filter list

- In the **Event Filter Configuration** dialog box, click and drag the Event Filter you want to reorder in the **Configured Filter List** to a new location in the list.

## Enabling and Disabling Event Filters

The configured Event Filter can be enabled or disabled using the parameter **enable** in the **event.filters** file located in the <Web NMS Home>/conf directory.

```
<EVENT_FILTERS>
<FILTER name="MyEventFilter" enable="true">
<FILTER_ACTION className=" com.adventnet.nms.eventdb.UserFilter"
name="userprop" userclass="com.adventnet.nms.eventdb.UserFilter" />
</FILTER>
</EVENT_FILTERS>
```

If the **enable** value is set to **true** (default value), the corresponding Filter is enabled; and if it is set to **false**, it is disabled.

**Note:** The enabling/disabling of Event Filter can done only by editing the **event.filters** file and not through the **Event Filter Configuration** tool.

## Deleting Event Filters

### To delete an Event Filter

1. In the **Event Filter Configuration** dialog box, select the Event Filter to be deleted from the **Configured Filter list**.
2. Click **Delete** in **Event Filter** section. A confirmation is asked.
3. Click **Yes** to delete the Event Filter.

### To delete an Action in an Event Filter

1. In the **Event Filter Configuration** dialog box, select the Event Filter in which the action is to be deleted from the **Configured Filter list**.
2. Select the action from **Configured Actions** list.
3. Click **Delete** in **Filter Action** section. A confirmation is asked.
4. Click **Yes** to delete the action for the Event Filter.

## 6.5.5 Configuring Alarm Filters

Events are correlated into alarms. They represent the current status of the existing problems in the network. An Alarm Filter executes certain corrective actions whenever alarms are received with configurable matching criteria, such as suppressing multiple alerts in a given interval, running shell commands on the server system, sending e-mails, sending traps, and running custom code to filter alerts.

Custom code may be needed in cases where any additional data has to be retrieved, or specific rules are to be applied in processing the alarm. Custom code is also the appropriate mechanism to configure alarm grouping, because it usually requires user or domain-specific rules that must be written for the specific application.

The processed alarms are stored in the database and made available in the Alarms Viewer. The Alarm Viewer is asynchronously notified, as soon as the processing of an alert is finished.

You can configure an Alarm Filter using the **Alert Filter Configuration** tool. You can use the properties of the event object in some of the fields, such as to Suppress Action, Run Command Action, Send Trap Action, and Send E-mail Action. For the list of the various event properties and their description, refer to Appendix.

A custom Filter can be configured to enable more effective event correlation and fault management by adding application-specific rules when processing events and alarms. However, this should be done by a developer and not by an administrator.

You can complete the following procedures when configuring Alarm Filters:

- Opening the Alarm Filter Configuration Tool
- Adding Alarm Filters
- Action Types
- Modifying Alarm Filters
- Saving Alarm Filter Files
- Loading Alarm Filter Files
- Reordering the Configured Alarm Filter List
- Enabling and Disabling Alarm Filters
- Deleting Alarm Filters
- Example

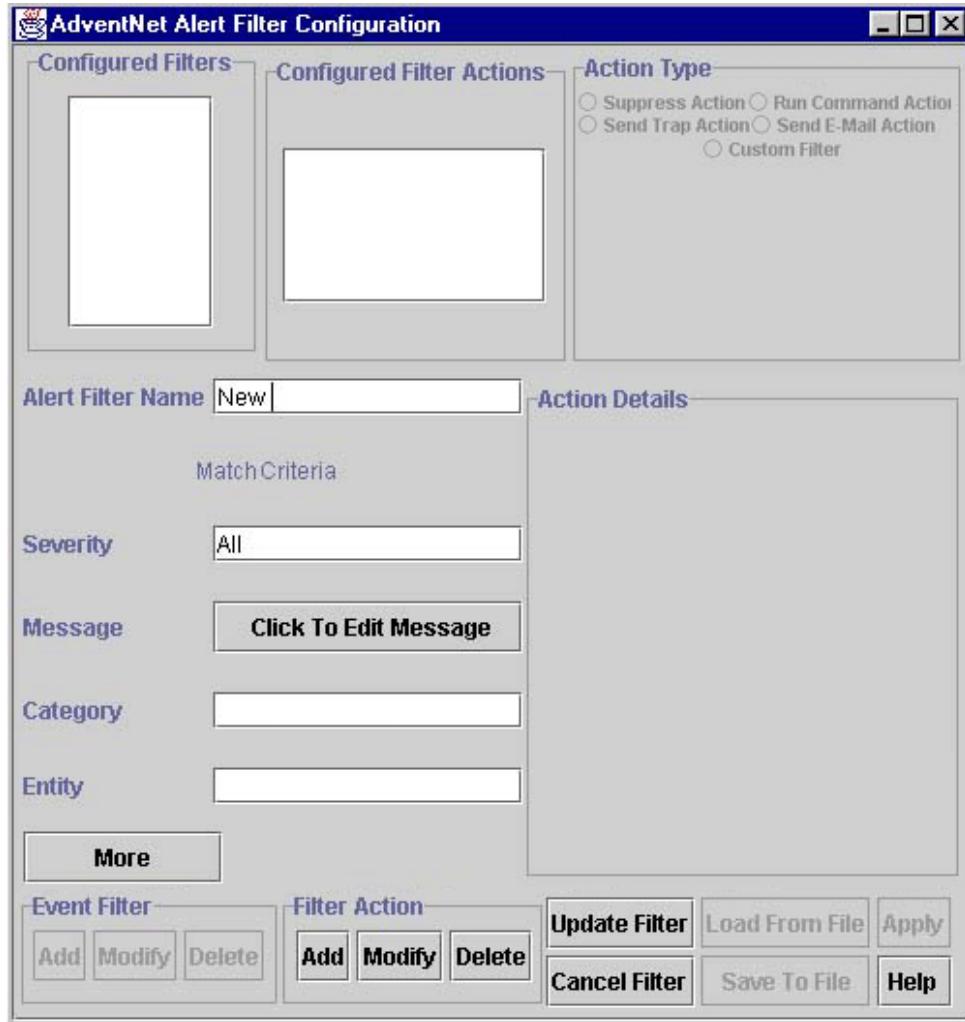
### Opening the Alarm Filter Configuration Tool

The Alarm Filters can be created or modified using the Alarm Filter Configuration tool.

#### To open the Alarm Filter Configuration Tool

- In the Web NMS Client, click **Fault Management > Alarms** node on the tree. From **Edit** menu, choose **Configure > Alarm Filters** or press **Ctrl+Shift+A**. Or
- In the Web NMS Launcher, from **Administrator Tools**, invoke **Alert Filter**. Or
- Execute the script file **AlertFilterAdmin** located in the **<Web NMS Home>/bin/admintools** directory.

The **Alert Filter Configuration** tool is displayed.



**Note:** The **Alert Filter Configuration** tool invoked from launcher or using script is an offline configuration tool. Hence it does not have the **Add To Server** option.

## Adding Alarm Filters

### To add an Alarm Filter

1. From the **Alert Filter Configuration** tool, click **Add**.
2. Specify a name for the Alarm Filter in **Filter Name** field.
3. Specify appropriate values as **Match Criteria**. For information on each of the Match Criteria fields, refer to the following table.

Field	Description
Severity	Match criteria based on the severity of the alarm, such as Critical, Major, and so on.
Message	Match criteria based on a message of the incoming alarm, such as Interface failure, Status Poll failed, and so on. Click <b>Click to edit message</b> . The <b>Alert Filter Message</b> dialog box is displayed. Specify the message.
Category	Match criteria based on an alarm object property with a category name to which the alarm belongs. This is used to organize alarms.
Entity	Match criteria based on the information about an exact device in which a problem has occurred.

The values that you specify in the Match Criteria determine whether the incoming alarm should be filtered. If this field is left blank, it is automatically matched. For the Alarm Filter to be applied, all the match criteria specified must be satisfied. If even one criterion fails, the Filter will not be applied. For information on the expressions and combinations that can be used while specifying the match criteria, refer to Configuring Event Filters topic.

To specify additional match criteria for the Alarm Filter, click **More** and complete the following steps.

- On clicking **More**, the **Alert Filter Configuration** dialog box is displayed.
- Specify the **Property Name** and **Match Criteria**. While specifying additional criteria, specify only those properties that are in the alarm object. The name should exactly match the case of the alarm object. You can also add alarm base properties as match criteria, such as **group name**, **help URL**, **ID**, and **time**. For more information on alarm properties, refer to Alarm Properties in Appendix.
- To add more properties, click **More**.
- When you are finished adding properties and values, click **OK**.

2. To include a filter action whenever the incoming alarm satisfies the match criteria, complete the following steps:
  - In the **Alert filter action** section, click **Add**. The **Action type** fields are enabled.
  - Choose one of the actions from Action type section. **Note:** An Alarm Filter must have at least one action associated with it.
  - Specify values for the selected action.
  - Click **Update action** to add the action to the configured actions list. The Update Action button toggles to the Update Filter button.
  - To add more actions, click **Add** and specify values for the selected action. At any time, to abort the adding of Filter or Action, click **Cancel filter** and **Cancel action** respectively.
5. When you are finished adding Filter and actions, click **Update filter**.
6. To save the configuration to the server, click **Apply**.

## Action Types

The action types that can be configured for an Alarm Filter are:

- Suppress Action
- Run Command Action
- Send Trap Action
- Send E-Mail Action
- Custom Filter

These action types are available while configuring the Alarm Filters. For information on each of these action types, refer to Action Types in Configuring Event Filters topic.

## Modifying Alarm Filters

### To modify Match Criteria of an Alarm Filter

1. In the **Alert Filter Configuration** dialog box, select the Alarm Filter to be modified, from **Configured filters** list.
2. Click **Modify** in **Alert filter** section. All the fields in the **Match criteria** section are enabled.
3. To specify your own properties to the alarm object generated by the Alarm Filter, click **More**. The **Alert filter configuration** dialog box is displayed.

Specify the name and value of the property in **Property Name** and **Match Criteria** fields respectively. To specify more properties, click **More**. When you are finished adding values and properties, click **OK**.

4. Make appropriate changes and click **Update filter**.
5. To apply this configuration to the server, click **Apply**.

### To modify Match Criteria of an Alarm Filter Action

1. In the **Alert Filter Configuration** dialog box, select the Alert Filter to be modified, from **Configured filters** list. Its corresponding actions are listed in **Configured filter actions** section.
2. Select the action.
3. Click **Modify** in **Alert filter action** section. All the fields in the **Action details** section are enabled.
4. Make appropriate changes and click **Update action**.
5. To apply this configuration to the server, click **Apply**.

## Saving Alarm Filter Files

### To save Alarm Filter files

1. In the **Alert Filter Configuration** dialog box, click **Save to file**. The **Save alert filters to file** dialog box is displayed.
2. By default, the configurations are saved in **alert.filters** file located in the <Web NMS Home>/conf directory. Specify a different filename, if required. The relative base directory for saving these files is the <Web NMS Home>.
3. Click **Save**.

## Loading Alarm Filter Files

Previously saved Alarm Filters can be loaded to the existing Filter list.

### To load an Alarm Filter file

1. In the **Alert Filter Configuration** dialog box, click **Load from file**. The **Load alert filters from file** dialog box is displayed.
2. Specify the filename.
3. Click **Load**.

**Note:** Any Filter with the same match criteria as that of the existing ones currently listed in the **Configured filters** list is replaced with the Alarm Filters from the file that you load.

## Reordering the Configured Alarm Filter List

### To reorder Alarm Filter list

- In the **Alert Filter Configuration** dialog box, click and drag the Alarm Filter you want to reorder in the **Configured filters** list to a new location in the list.

## Enabling and Disabling Alarm Filters

The configured Alarm Filter can be enabled or disabled using the parameter **enable** in the **alert.filters** file located in the <Web NMS Home>/conf directory.

```
<ALERT_FILTERS>
<FILTER enable="true" name="FilterName">
<FILTER_ACTION className="com.adventnet.nms.eventdb.UserFilter"
name="EXAMPLE" userclass="com.adventnet.nms.eventdb.UserFilter" />
</FILTER>
</ALERT_FILTERS>
```

If the **enable** value is set **true** (default value), the corresponding Filter is enabled; and if it is set **false**, it is disabled.

**Note:** The enabling/disabling of Alarm Filter can be done only by editing the **alert.filters** file and not through the **Alert Filter Configuration** tool.

## Deleting Alarm Filters

### To delete an Alarm Filter

- In the **Alert Filter Configuration** dialog box, select the Alarm Filter to be deleted from the **Configured filter** list.
- Click **Delete** in **Alert filter** section. A confirmation is asked.
- Click **Yes** to delete the Alarm Filter.

### To delete an Action in an Alarm Filter

- In the **Alert Filter Configuration** dialog box, select the Alarm Filter in which the action is to be deleted from the **Configured filters** list.
- Select the action from **Configured filter actions** list.
- Click **Delete** in **Alert filter action** section. A confirmation is asked.
- Click **Yes** to delete the action configured for the Alarm Filter.

## Example

An example where you need to send an e-mail to the manager with the message in the body as "*An Alert of Category <CATEGORY> and severity <SEVERITY> has been generated from <SOURCE>. It has been picked up by <OPERATOR>.*"

Also, an Alarm is generated with the following properties (the alarm will have many other properties which are not taken for consideration in this example).

S.No.	Property Name	Property Value
1	category	general
2	severity	1
3	source	printer1
4	who	james

## Procedure

1. In the Alert Configuration tool, click **Add** in **Alert filter** section.
2. In **Filter Name** field, specify **example**.
3. In **Severity** field, specify **1**.
4. In **Category** field, specify **general**.
5. Click **More**. The **Alert Filter Configuration** dialog box is displayed.
6. Specify **source** and **printer1** in **Property Name** and **Match Criteria** fields respectively.
7. Click **More**.
8. Specify **who** and **james** in **Property Name** and **Match Criteria** fields respectively.
9. Select both the options.
10. Click **OK**.
11. Click **Add** in **Alert filter action** section.
12. Select **Send e-mail action** in **Action type** section.
13. In **Send E-mail Action Name** field, specify **examplemail**.
14. Specify appropriate values for remaining fields.
15. In the **Message** field, specify "*An Alert of Category \$category and severity \$severity has been generated from \$source and has been picked up by \$who*".

On executing this example, a mail is sent for this type of alarm and it has the following message in the body of the e-mail:

*"An Alert of Category **general** and severity **1** has been generated from **printer1** and has been picked up by **james**"*

## 6.5.6 Performing Alarm Operations

The administrative tasks that you can perform in the Alarm View are

- Clearing Alarms
- Deleting Alarms
- Grouping Alarms
- Printing Alarms

### Clearing Alarms

The alarms that are generated in the network are automatically cleared during runtime. You can also clear an alarm manually, when it has been resolved or if it is inconsequential. Sometimes, the agent sends fault only when there is a crisis and does not send notifications when that crisis is resolved. In such a scenario, you can manually clear the alarm.

#### To clear an alarm

1. Open the Alarm Viewer.
2. Select the alarm to be cleared by clicking the corresponding row.
3. From Edit menu, choose **Clear** or press **Ctrl+L**.

### Deleting Alarms

You have an option to delete an alarm when you feel the alarm is not significant or the alarm has been cleared. By default, the alarms that are in Clear status for more than 24 hours are deleted and this deletion happens every 60 minutes automatically. But if you want to manually delete the cleared alarms, use this option.

#### To delete an alarm

1. Open the Alarm Viewer.
2. Select the alarm to be deleted by clicking the corresponding row.
3. From Edit menu, choose **Delete** or press **Ctrl+R**.
4. A confirmation is asked. Click **OK**.

### Grouping Alarms

For ease of administration, you can group the alarms based on some criteria. For example, you can group all the alarms pertaining to a single device and represent them as a single unit.

The grouped alarms are depicted as a single representative in the Client. This representative is based on the value specified for the **groupName** field present in the Events and Alarms views.

For this grouping to be possible

- In the **Trap Parser Configuration** tool, set a value to the **Group Name** field - This will set the Group Name as specified here for all the Events which are generated by this Trap Parser.
- In the **Event Parser Configuration** tool, click the **More** button. In the Properties dialog box,
  - Set the **Field Name** as **groupName**.
  - Set the **Output String** with the **<name of the group>**.
  - Leave the **Match String** and the **Tokenizer String** columns empty.

This will set the group name as specified here for all the Events which pass through this Event Parser.



**Warning:** When you specify the value for **GroupViewMode** in Alarms Custom View, the FE Server fetches the data from the database for every alarm that is received. The FE Server will not maintain the details of all the alarms in a group and hence fetches the data from the database. This degrades the performance of the server.

## Printing Alarms

By default, the print option for Events and Alarms in Web NMS Client is not configured. To enable printing, configuration has to be done in **NmsProcessesBE.conf** file located in <Web NMS Home>/conf directory. For more information on editing this file, refer to Print Option in Developer Guide.

## 6.5.7 Setting User Privileges

You can restrict a user from accessing certain data in the Web NMS Client and also confine him to viewing and working only on selected network events and alarms. This is achieved using the **Custom View Scope** mechanism of the Security Management. For more information, refer to Managing Custom View Scopes.

This topic provides an example based on which you can create your own Custom View Scopes.

### Example

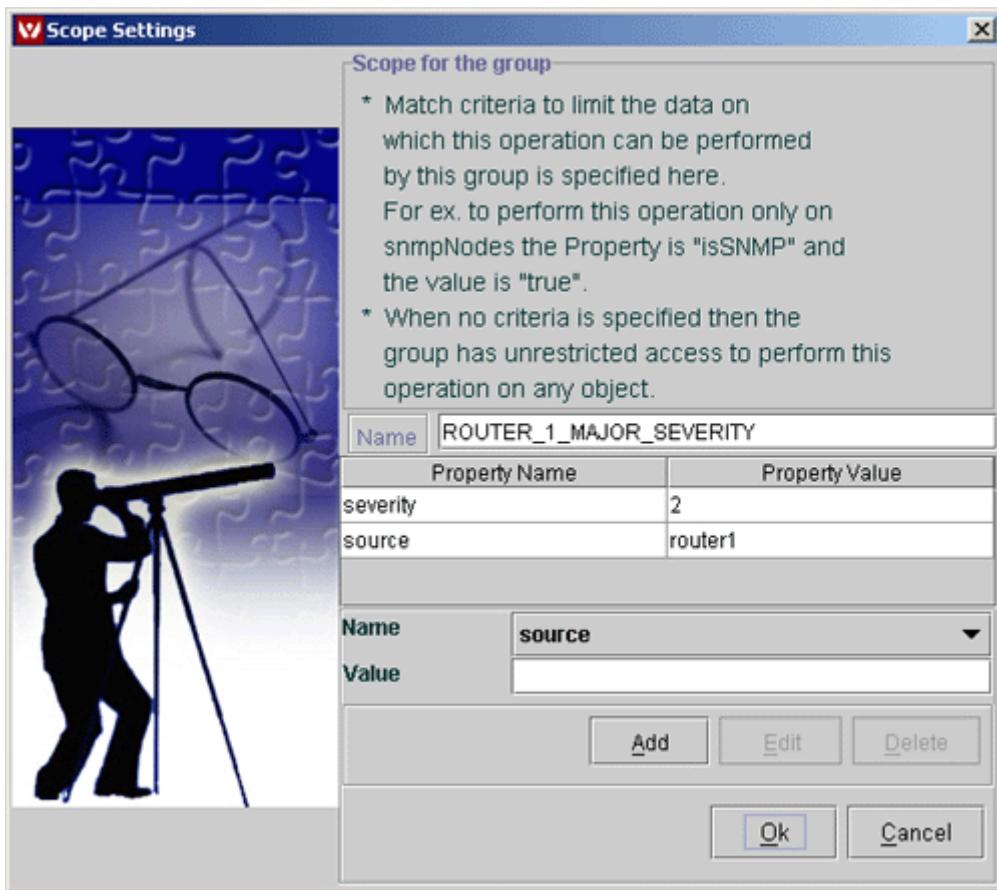
This example aims at

- Creating a user named **test**.
- Associating this user with a new group named **faultgroup**.
- Providing **faultgroup**, the permission to view and perform operations on alarms from a specific network element named **router1** and with an alarm severity of **Major**.

### Procedure

1. In Web NMS Client, from **Tools** menu, choose **Security Administration**. The **Security Administration** tool is displayed.
2. Add a new user named **test**.
3. Add a new group named **faultgroup**.
4. Assign required permissions to the **faultgroup**.
5. Assign the new user **test** to the **faultgroup**.
6. Set the Scope Criteria.
  - Select the **faultgroup** on the **Security** tree.
  - Click **Custom View Scope for Group** tab on the right-side frame.
  - From **Custom View Scope for Group** drop-down box, choose **Alerts**.
  - Click **Add AuthorizedScope**. The **Scope Settings** dialog box is displayed. Enter the **Name** as **Router1\_Major**. From **Name** drop-down box, choose the property as **severity** and enter the **Value** as **2**. For information on each of the properties listed in the **Name** drop-down box, refer to Appendix in User Guide.
  - Click **Add**.
  - Again, from **Name** drop-down box, choose the property as **source** and enter the **Value** as **router1**.
  - Click **Add**.
  - Click **OK**.
7. Click **Permitted Operations for Group** tab.

A screen shot depicting the procedure is given below.



### Result

When you log in with user name **test**, you will be able to view only the alarms of the network element **router1** with **Major** severity.

## 6.5.8 Configurable Parameters

The Fault Management module can be administered by configuring the following parameters in **EventMgr** process in the **NmsProcessesBE.conf** file located in <Web NMS Home>/conf directory.



**Note:** If you have configured any of the parameters, ensure to restart the Web NMS Server.

The parameters that can be configured by administrators are listed below. For information on the above parameters, refer to Configuring Event Parameters topic in Developer Guide.

- To save events/alarms - SAVE\_DIR
- To print events/alarms - PRINT\_COMMAND
- To delete events - CLEAN\_EVENT\_INTERVAL
- To control the number of events to be managed by Web NMS - EVENT\_WINDOW\_SIZE
- To drop traps from unmanaged objects - DROP\_TRAP\_WHILE\_UNMANAGED
- To enable authorization - AUTHORIZATION
- To enable authentication - V3\_AUTH
- To acknowledge inform requests - NEED\_INFORM\_ACK
- To delete clear alarms - ALERT\_DELETE\_INTERVAL
- To update MO with respect to the alarm - ALERT\_TO\_MANAGEDOBJECT\_PROPAGATION
- To group Alarms - GROUP\_ALERTS\_MODE
- To control the number of alarms to be managed by Web NMS - ALERT\_WINDOW\_SIZE
- To create alarm history objects - CREATE\_ALERT\_HISTORY
- To remove annotations on deleting alarms - ON\_DELETING\_ALERT\_DELETE
- To remove alarms on deleting MO - ACTION\_ON\_DELETING\_MO

## 6.6 Configuration Management

Configuration Management deals with configuring devices in the network to achieve a defined functionality and this can be performed using **Tasks** in Web NMS. **Task** is an entity that contains all the configuration details that are needed to configure a device. It comprises the task-level information and the attributes to be configured.

### To perform task-related operations

1. Open the Web NMS Client
2. On the left-side tree, click **Configuration > Batch Configuration**. The **Batch Configuration** panel is displayed on the right-side frame.

Task Name	Task Description	Protocol	Templ...	Rollb...	Last Execut...
AcmeCardConfiguration	This task is used for c...TL1	false			Not Executed
BroadCastStormControl	This task configures t... TELNET	true			Not Executed
CiscoAccessListDeletion	This task is used to re... TELNET	true			Not Executed
CiscoAccessListGener...	This task is used to c... TELNET	true			Not Executed
CiscoConfigBackup	This task is used for t... TELNET	true			Not Executed
FileTransfer	This task is used for t... TFTP	false			Not Executed
NATAddition	This task adds an entr... TELNET	true			Not Executed
NATRemoval	This task is used to re... TELNET	true			Not Executed
NetworkDiscovery	This task is used for d...SNMP	true			Not Executed
RouteAdd	This task adds a route...TELNET	true			Not Executed
RouteDelete	This task deletes the ... TELNET	true			Not Executed
SystemDateConfiguration	This task is used for c...TL1	false			Not Executed
SystemGroupConfigura...	This task is used for c...SNMP	false			Not Executed
TrapForwarder	This task is used for f... SNMP	true			Not Executed

Done.

In this panel, you can view all the default Tasks configured in the Web NMS. This chapter explains the various other operations you can perform using Tasks.

- 
- Configuring Tasks
  - Reusable Tasks
  - Creating Device Lists
  - Executing Tasks
  - Executing Default Tasks
  - Auditing
  - Configurable Parameters
-

## 6.6.1 Configuring Tasks

Before creating a Task to configure devices in the network, you need to know the following information:

- The variables (attributes or OIDs) to be configured
- The values to be set for the variables
- The protocol to be used for configuring the device

Once this information is determined, you can create a new Task.

---

- Adding a New Task
    - Defining Variables
      - SNMP
      - Telnet
      - TFTP and FTP
      - TL1
  - Configuring Rollback for Tasks
  - Creating Combined Tasks
  - Modifying a Task
  - Deleting a Task
- 

### Adding a New Task

To add a new Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**.
2. From **Config Operations** menu, choose **Task Operations > Add Task** or press **Alt+A**. The **Task Configuration** wizard is displayed.
3. Enter a name for the Task in **Name of the Task** field (mandatory). **Example:** snmptask
4. Enter a brief description of the Task that you are creating in **Task Description**. **Example:** Task for setting the OIDs
5. Select the protocol on which the Task is based, from the **Protocol Information** panel.
6. Select **Define as Template?** option if required. For information on this field, refer to Reusable Tasks topic.
7. Click **Next** to define the attributes/variables. The next screen differs based on the chosen protocol. For information on each of the screens, refer to the next section Defining Variables. Enter values for the subsequent screens.
8. In the final screen (which has the **Finish** button), enable the **Rollback** facility if required. For more information on Rollback, refer to Configuring Rollback for Tasks.
9. After configuring the fields in the subsequent screens, click **Finish**.

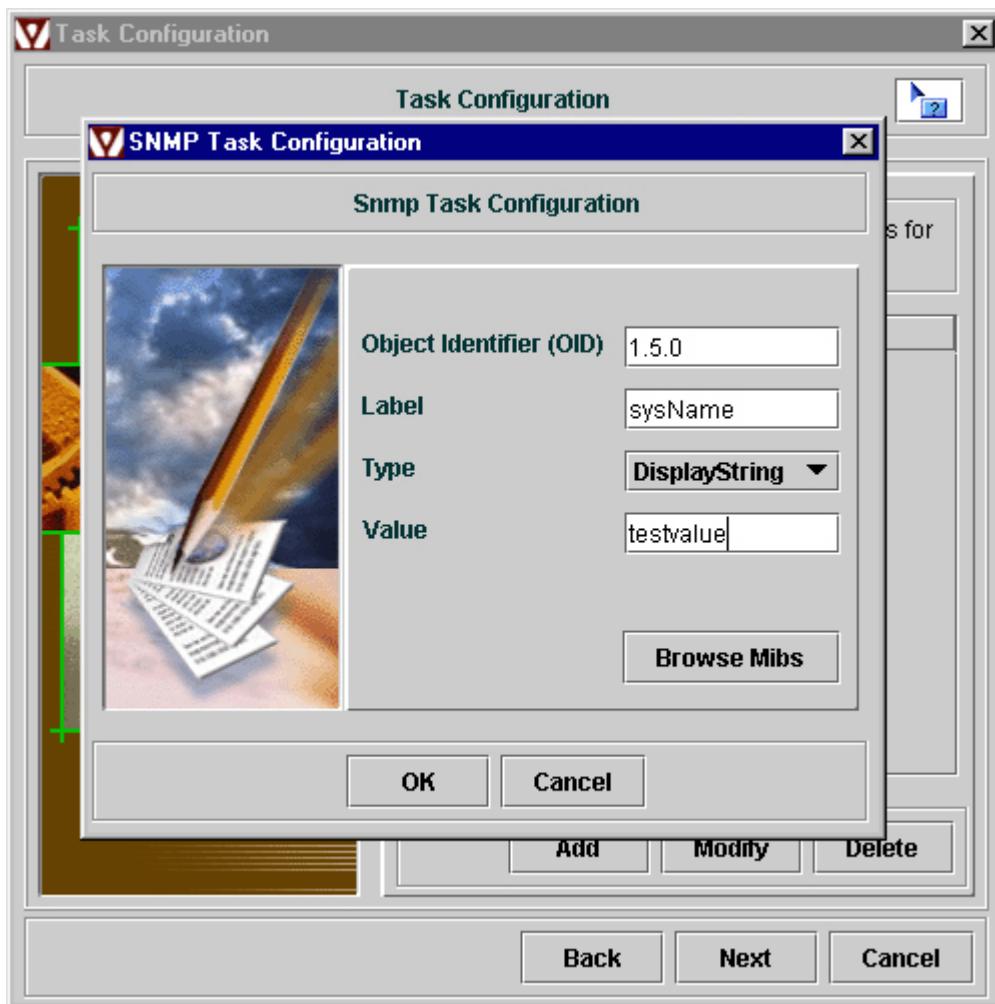
## Defining Variables

This section explains the screens that are displayed based on the chosen protocol.

### SNMP Variables

If you had chosen **SNMP**, continue to execute the following procedure.

Three type of attributes can to be configured for a task when SNMP is selected, namely **Scalar Attribute**, **Columnar Attribute**, and **Table Attribute**. You can complete the configuration for all three attributes or at least a single attribute.



- After performing steps 1 to 7 as explained in To add a new task section, in the next screen, click **Add**. The **SNMP Task Configuration** dialog box is displayed.
- Configuring Scalar Attribute:** The initial screen displays the **Scalar Attributes** (OID, Label, Type, and Value). Enter the values manually in the respective fields or simply browse through the MIBs.

#### Entering the Scalar Attributes manually

- Enter the OID in **Object Identifier (OID)** field. Complete OID can be specified. If the value that you specify is not preceded with a dot (.), then, by default, .1.3.6.1.2.1, is prefixed with the OID that you specify.
- Enter the label for the OID in **Label** field.

- Choose the type of the OID from the **Type** drop-down box.
- Enter the value that has to be set for the OID, when the specified device is configured in **Value** field.

#### Browse MIBs

Instead of entering values manually, you can configure them using the MIB.

- Click **Browse Mibs**. The **Browse MIBs** dialog box is displayed.
- Click **Load** to load the MIB file from which you need to specify the Scalar Attributes.
- Browse through the MIB tree and select the required OID.
- Click **Select**. The **OID**, **Label**, and **Type** values are configured automatically.
- Enter the **Value**.

On entering the Scalar Attributes, click **OK**. You can add more than one Scalar Attributes by performing the same procedure.

**3. Configuring Columnar Attributes:** To configure only **Columnar Attributes**, skip step 2 and perform the following procedure.

- In the **SNMP Task Configuration** dialog box, click **Browse Mibs**. The **Browse MIBs** dialog box is displayed.
- From the MIBs tree, choose an OID from a table.
- Click **Select**. A confirmation message prompting you to define the index value for the table to which the columnar OID belongs is displayed. Click **Yes**. The **SNMP Task Configuration** dialog box is displayed. If you click **No**, you cannot add complete the operation of adding Columnar Attributes.
- Select the OID on the table and enter the table index value for the OID in **Value** field and click **Update**.
- Click **OK**. You can add more than one Columnar Attribute by performing the same procedure.
- Click **Next** to add **Tabular Attribute**, if required.

**4. Configuring Tabular Attribute:** To configure only Tabular Attributes, skip steps 2 and 3 and perform the following procedure.

0. Click **Add Table** in the next screen (after Scalar Attribute screen). The **Browse MIBs** dialog box is displayed.
1. Select the table from the MIBs tree. Click **Select**. The table is added and the columns in that table which are configurable are listed on the right-side frame. Now, you can either add new rows to the table or modify/delete existing rows.
2. To add a new row, click **Add Row**. The **SNMP Task Configuration** dialog box is displayed. Select each of the OIDs on the table, enter the value, and click **Update**. The values given for the columns should be compatible with their data types. The data type of the column can be known from the MIB.
3. Click **Next** when done.

## Telnet Variables

If you had chosen **Telnet**, continue to execute the following procedure.

1. After performing steps 1 to 7 as explained in To add a new task section, in the next screen, click **Add**. The **Telnet Task Configuration** dialog box is displayed.
2. In the **Command** field, specify the command that needs to be executed on the device. For example, if you want to execute **Is** command on the device, then specify the command in this field.
3. In the **Command Arguments** field, specify the arguments, if any, for the command to be executed. If **Is -I** command has to be executed, then **-I** is the argument for the **Is** command. Note that a space has to be added before the command line argument.
4. In the **Prompt** field, specify the telnet prompt of the device under configuration. The command will be executed on the device, only if the device prompt is the same as specified in this field.
5. Click **OK**.

## TFTP and FTP Variables

If you had chosen **TFTP/FTP**, continue to execute the following procedure.

1. After performing steps 1 to 7 as explained in To add a new task section, in the next screen, click **Add**. The **TFTP/FTP Task Configuration** dialog box is displayed.
2. In the **Source** field, specify the name of the file that needs to be transferred. Ensure that the filename specified in this field is case sensitive.
3. In the **Destination** field, specify the name in which the file should be stored after transfer. The destination filename can be the same as that of the source name or a different name. If the destination filename is not specified, it will be stored in the same name as that of the source filename. Ensure that the filename specified is case-sensitive.
4. In the **Mode** field, choose the mode **ASCII** or **Binary** using which the file should be transferred between machines. Specify **Binary** mode when the file format is other than ASCII text (including zip or image files).
5. In the **Command** field, choose the command **Get** or **Put**. To transfer a file from local machine to another destination machine, choose **Put**. To get a file from another machine to the local machine, choose **Get**.
6. Click **OK**.

## TL1 Variables

If you had chosen **TL1**, continue to execute the following procedure.

1. After performing steps 1 to 7 as explained in To add a new task section, in the next screen, click **Add**. The **TL1 Task Configuration** dialog box is displayed.
2. In the **Command Code** field, specify the command to be executed over the TL1 device.
3. In the **Target ID** field, specify the ID that is used to associate the message with the network element, or one or more intermediate network elements.
4. In the **Access ID** field, specify an ID that is used to identify the entity with the target ID.
5. In the **General Block** field, specify the support parameters that affect the way in which an input command is executed by the network element.
6. In the **Message Payload Block** field, specify the data in block.
7. Click **OK**.

## Configuring Rollback for Tasks

When a task is submitted for execution, the task may fail if the device is unreachable or OID not present or the OIDs cannot be configured or any other reason. In such cases, the older values are to be reverted to the device. This can be done in two ways.

- **Current Configuration:** When this is used, the older values are fetched from the device, before configuring the device. If the configuration fails, the older values are reverted.
- **Rollback Document:** In this case, some other task is associated with the primary task that will be executed on the device, if the primary task fails.

To configure for Current Configuration

1. In the final screen (where **Finish** button is available) of the Task Configuration Wizard, click the **Use Current configuration for Rollback** check box.
2. Click **Finish**.

On performing this, when a task fails during execution, the variable that was to be modified in the device is restored with the old value.

To configure for Rollback Document

1. In the final screen (where **Finish** button is available) of the Task Configuration Wizard, click the check box of the task from **Available Tasks For Rollback** section.
2. Click **Finish**.

On performing this, when a task fails during execution, the task that is configured for Rollback is performed.

## Creating Combined Tasks

Combined Task is a collection of two or more sub-tasks which can belong to any protocol. This section explains how you can create a combined task using already existing tasks, say task1, task2, and task3.

To create combined tasks

1. In the Web NMS Client, under Configuration Management, from **Config Operations**, choose **Task Operations > Add Task** or press **Alt+A**. The **Task Configuration** wizard is displayed.
2. Enter the task name and task description in **Name of the Task** and **Task Description** fields respectively.
3. In the **Protocol Information**, select **Combined Task**.
4. Click **Next**. The **Combined Task Panel** is displayed with the existing configured tasks.
5. In the **Available Sub-Task**, under each of the protocols node, the existing tasks are displayed. Select the check box of each of the tasks that you need to configure as a part of the combined task. **Note:** Template tasks cannot act as sub-tasks for a combined task.
6. Click **Finish**.

On performing this, whenever this combined task is executed, all the sub-tasks associated with this task are also executed.

## Modifying a Task

### To modify a task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All tasks are displayed on the right-side panel.
2. Select the task that you need to edit on the right-side panel.
3. From **Config Operations** and choose **Task Operations > Modify Task** or press **Alt+M**. The **Task Configuration** wizard with the configuration information is displayed.
4. Make required modifications and click **Finish** (in the final screen).

## Deleting a Task

### To delete a task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All tasks are displayed on the right-side panel.
2. Select the task that you need to delete on the right-side panel.
3. From **Config Operations** and choose **Task Operations > Remove Task** or press **Alt+R**. A confirmation is asked.
4. Click **Yes** to delete the task.

## 6.6.2 Reusable Tasks

The data used for configuring devices consists of the attributes to be configured and the values to be set for those attributes. You need to create tasks, one for each device, with different values for the attribute. This becomes tedious if there are more number of devices to be configured. This can be solved by creating **Reusable Tasks**.

Reusable Tasks are technically called **Template Tasks**. Template tasks can be reused to configure multiple devices, just by changing the values for the attributes to be configured. The values for each attribute for a device can be specified separately in a data source, that forms the central repository of data, while the task is executed.

- Creating Template Tasks
- Creating Data Source

### Creating Template Tasks

Template Task contains place holders as the values of the attributes. When the Task is executed, these place holders are replaced with the values extracted from the data source. The four different types of place holders are:

- **InventoryInput:** This placeholder can be used whenever you intend to fill the placeholder with the values got from the Managed Object database. To use this type, the values for the attributes are to be present in the database against the device being configured.
- **NEInput:** This placeholder can be used when you want to fetch the values from a network element and fill the placeholder. In this case, the network element will be contacted and the value returned by that element will be substituted.
- **UserInput:** This place holder can be used when you want to set values for the place holders, before hand, by hard coding it in the data source.
- **DataSourceParam:** This place holder can be used if you want to get the values for this place holder from the user at the time of execution of the task.

#### To create a Template Task

The procedure to create a template task is the same as the procedure explained in Adding a New Task. In the **Task Configuration** wizard, select the option **Define as Template?**.

On selecting this option, in further screens, the following two fields are available:

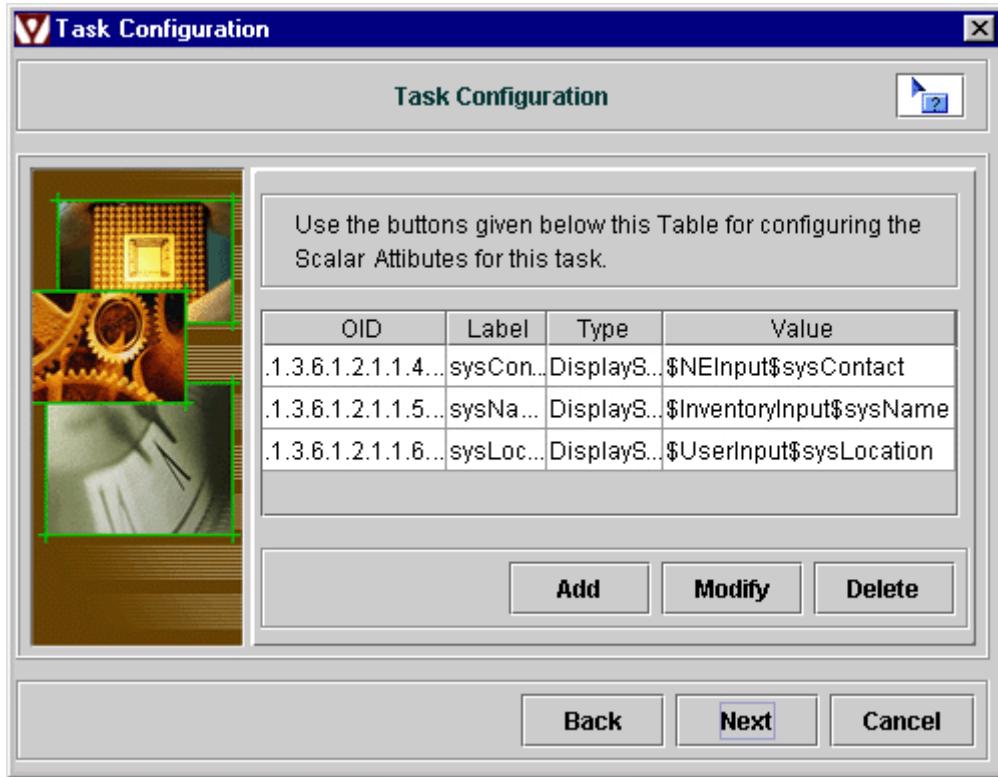
- **Type:** Choose the type of place holder from this drop-down box.
- **Place Holder:** Specify a variable to identify the type. It is suggested to retain the same value as the Label field.

### Creating Data Source

Data Source is a central repository that supplies data input to the place holders of the Template Task. Whenever the Template Task is executed, values are taken from the Data Source and filled up for the attributes of the Template Task.

This section explains the procedure to create Data Source using an example.

Assume, there exists a template task with attributes as shown in the image:



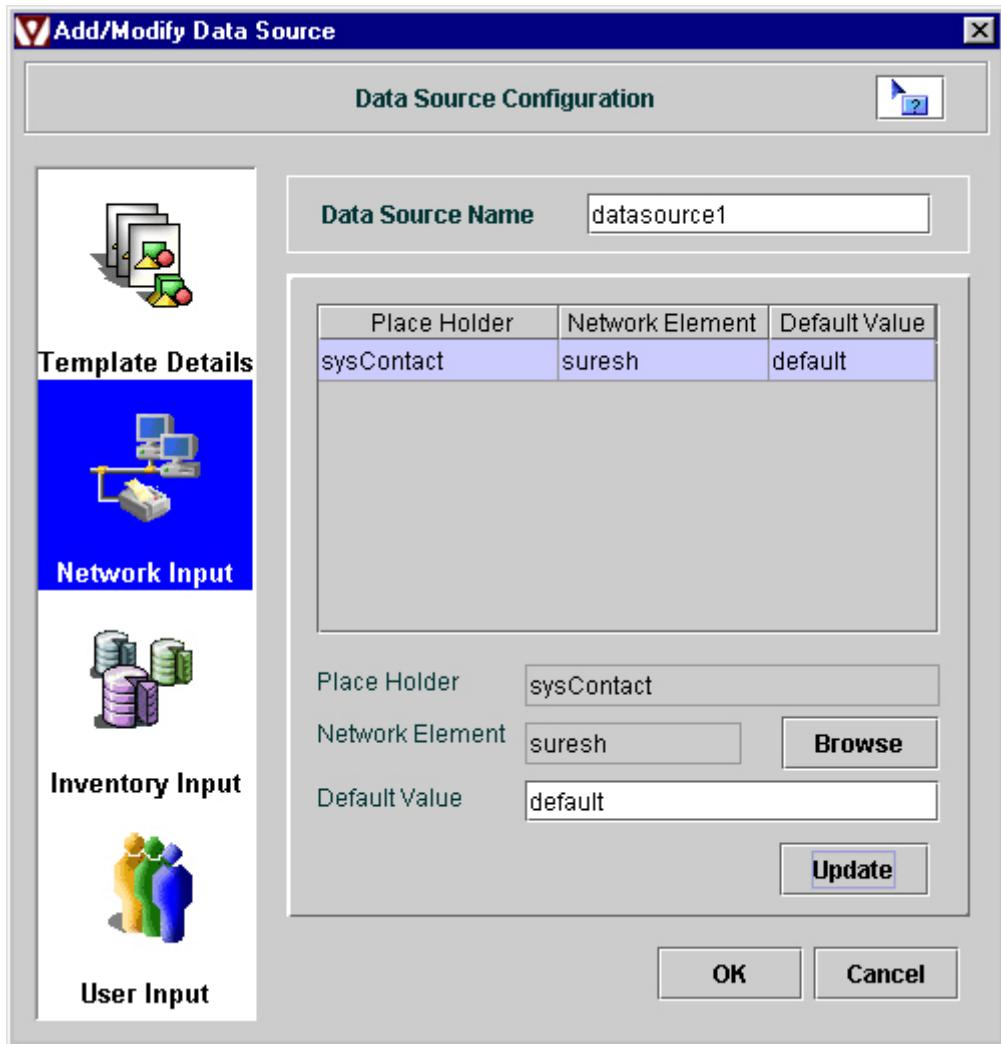
Let us create a Data Source that will supply inputs to each of the place holders namely, **\$NEInput\$sysContact**, **\$InventoryInput\$sysName**, and **\$UserInput\$sysLocation**.

#### To create a Data Source

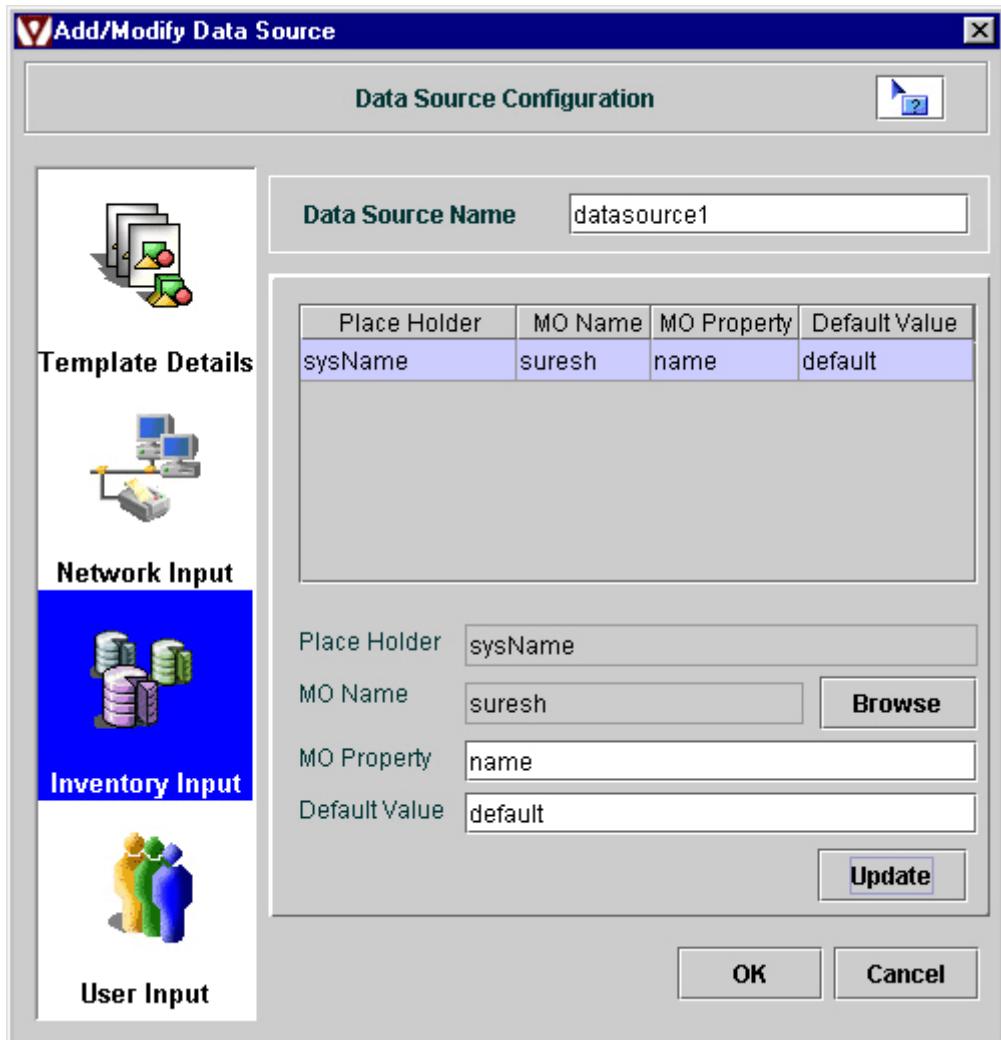
1. In the Web NMS Client, click **Configuration > Batch Configuration**.
2. From **Config Operations** menu, choose **Data Source Operations** or press **Ctrl+S**. The **Data Source Configuration** dialog box is displayed.
3. Click **Add**. The **Add/Modify Data Source** dialog box is displayed.
4. Specify a name for the Data Source in the **Data Source Name** field. **Example:** newdatasource

In further steps, values should be specified for all the three types of place holders that were created earlier.

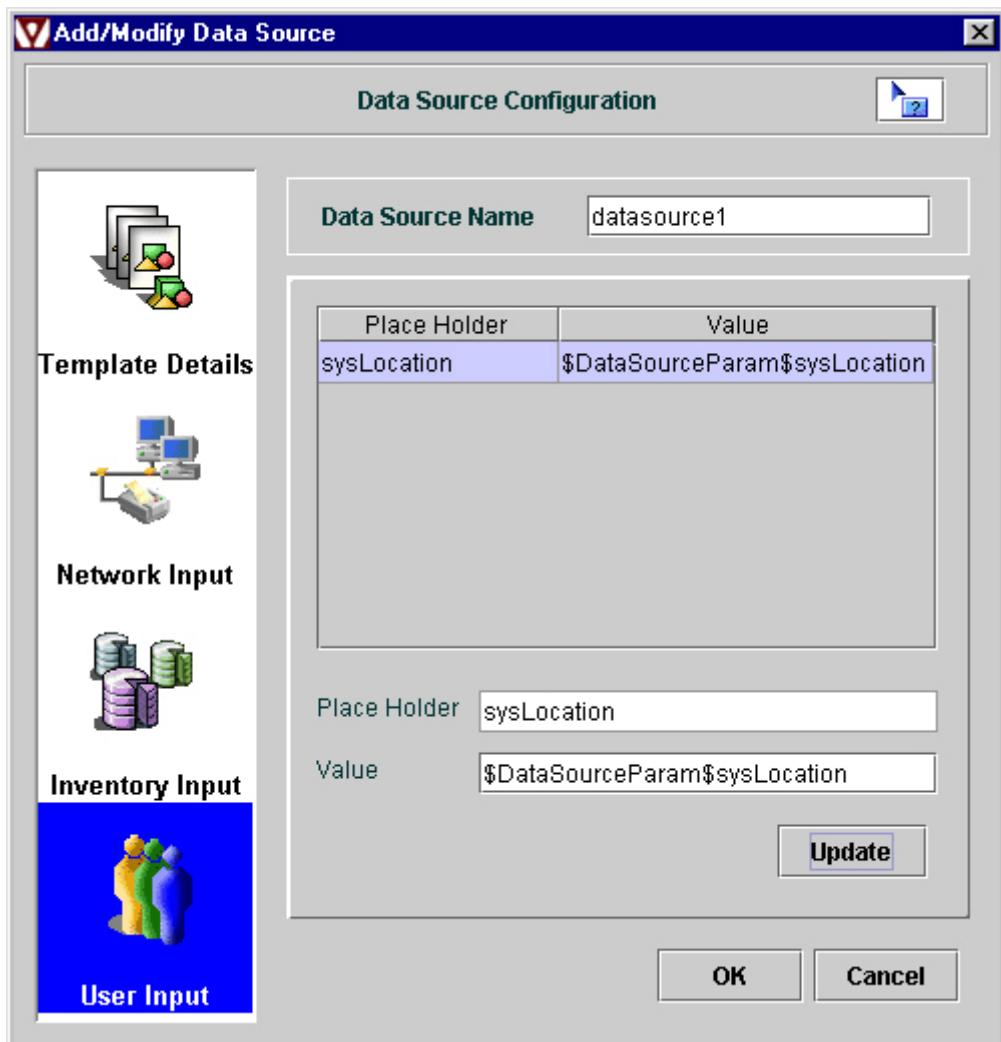
5. Click **Network Input** icon on the left side of the **Data Source Operations** dialog box.
  - Click **Browse**. The **Select Device** dialog box is displayed.
  - Specify the device name in the **Add Devices** field and click **Add**. The device is added to the **Devices** table and its details are listed in the **Devices Attributes** table. You can also locate a device using the **Search** option.
  - To change values of the attributes, select the attribute on the table, change the value in **Value** field and click **Update**.
  - Click **OK**.
  - Specify the default value in **Default Value** field. This value is substituted for the place holder, if the device is not available or could not be contacted.



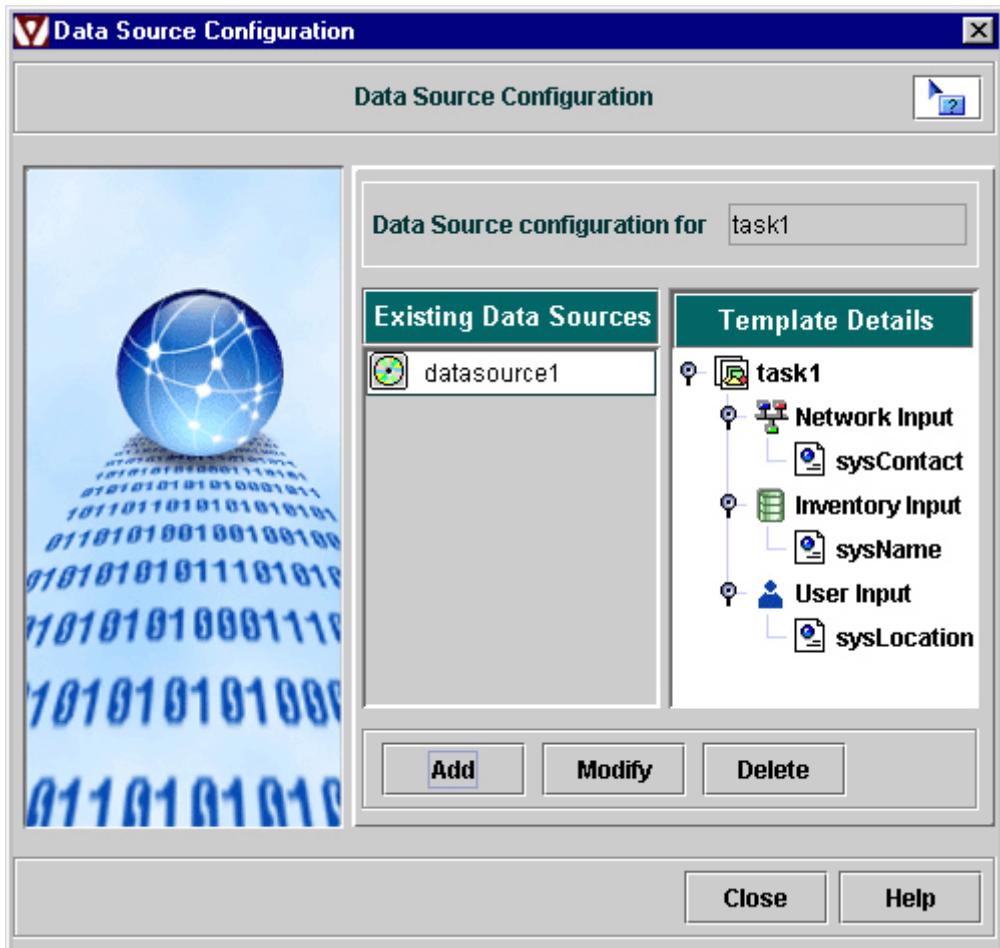
6. Click **Inventory Input** icon on the left side of the **Data Source Operations** dialog box.
  - Click **Browse**. The **Select Device** dialog box is displayed.
  - Specify the device name in the **Add Devices** field and click **Add**. The device is added to the **Devices** table and its details are listed in the **Devices Attributes** table. You can also locate a device using the **Search** option.
  - To change values of the attributes, select the attribute on the table, change the value in **Value** field and click **Update**.
  - Click **OK**.
  - Specify the default value in **Default Value** field. This value is substituted for the place holder, if the device is not available or could not be contacted.



7. Click **User Input** icon on the left side of the **Data Source Operations** dialog box. As it is a user input whose value should be provided at the time of execution of the template task, you can use the **DataSourceParam** place holder.



8. Click **OK**. The newly created Data Source is listed in the **Existing Data Sources** table.

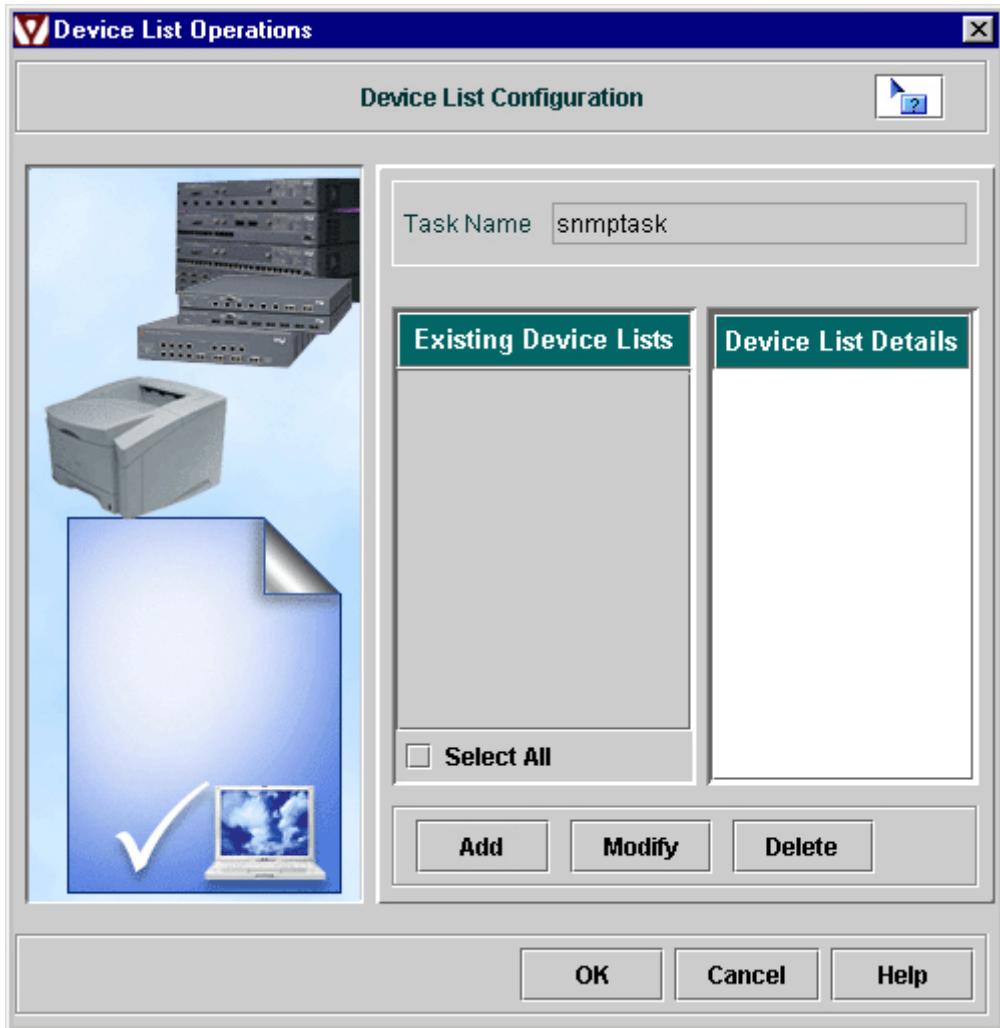


9. Click **Close** to finish the Data Source Configuration operation.

Henceforth, whenever the Template Task is executed, the values are taken from this Data Source and executed.

## 6.6.3 Creating Device Lists

A **Device List** is a logical collection of devices. When a task is to be executed over, say 10 devices, then you can create a Device List with those 10 devices and associate it with the task.



### To create a Device List

1. In the Web NMS Client, click **Configuration > Batch Configuration**.
2. Select a task on the right-side panel.
3. From **Config Operations** menu, choose **Device List Operations** or press **Alt+D**. The **Device List Operations** dialog box is displayed.
4. Click **Add** to create a new Device List. The **Add/Modify Device List** dialog box is displayed.
5. Specify a name for the Device List in **Device List Name** field.
6. Enter the name of device in **Enter Device Name** field. Click **Add**. You can add as many device names as required for the Device List.

You can also specify the device names by performing a search operation. On using search option, you can list a set of devices satisfying a specific criteria. This saves time on entering devices names individually.

**7. To search for a device**

- Click **Search Device**. The **Search For Devices** dialog box is displayed.
  - Using the Search Criteria specify appropriate values. **Example:** Name starts with 'a'. For more criteria, click **More**.
  - Click **Search**. All devices satisfying the search criteria are displayed in the **Device Names** section of the **Add/Modify Device List** dialog box.
  - Select the check boxes (if not selected already) of those devices that you need to add to the Device List.
8. Click **Next**. All devices and their properties are listed in the next screen.
9. Click **>>** to view a device's details.
10. To edit the properties, select the device and click **Edit Properties**. The **Device Attributes** dialog box is displayed. Select the Property Name on the table, modify the value in **Value** field and click **Update**. Click **Done**.
11. Click **Finish**.

Now, when you execute a task with this Device List associated, the configuration is applied over all the devices in the Device List.

## 6.6.4 Executing Tasks

Once the tasks are created for configuring the devices, the devices have to be associated with the task before it is executed. The procedure to execute an ordinary Task and a reusable Template Task differs. This topic explains the procedure to associate devices with the tasks and to execute them.

- Executing Tasks
- Executing Template Tasks
- Executing Combined Tasks
- Executing Telnet Tasks
- Uploading Configuration from Device

### Executing Tasks

#### To execute a task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the Task to be executed on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed. The Device List table lists the devices (if exists for the Task).
4. Select **Would you like to associate devices for this task** to associate devices with the Task.
5. Click **Next**.
6. Use the **Search** option to locate the device to be configured. If found, the device is displayed in the **List of Devices** table. The device information is displayed in the **Device Attributes** table. Select the device. To change the value of any attribute, select the attribute, specify the new value in the **Value** field, and click **Update**.
7. Click **Next**. The devices available for the task execution are displayed.
8. Click **Finish** to start the configuration.

Once the task is executed, the time of execution is updated in the **Batch Configuration** panel. You can view the task audit details to know the attributes that have been configured.

### Executing Template Tasks

The procedure to execute a Template Task differs from that of an ordinary task.

#### To execute a Template Task

**Note:** Ensure to create the Data Source before executing a Template Task.

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the Template Task to be executed on the **Batch Configuration** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed. The Device List table lists the devices (if exists for the Task).
4. Select the Data Source from the **Available Data Sources** table.

5. Click **Configure Data Source Parameters**. (**Note:** This button is enabled only when a User Input type of place holder is created. Otherwise, skip this step.). The **Configure Data Source Parameters** dialog box is displayed. Specify value for the parameter and click **Update**. When the values are specified, click **OK**.
6. Click **Next**.
7. Select **Would you like to associate devices for this task** to associate devices with the Task.
8. Click **Next**.
9. Use the **Search** option to locate the device to be configured. If found, the device is displayed in the **List of Devices** table. The device information is displayed in the **Device Attributes** table. Select the device. To change the value of any attribute, select the attribute, specify the new value in the **Value** field, and click **Update**.
10. Click **Next**. The devices available for the task execution are displayed.
11. Click **Finish** to start the configuration.

Once the task is executed, the time of execution is updated in the **Batch Configuration** panel. You can view the task audit details to know the attributes that have been configured.

## Executing Combined Tasks

Combined Tasks is a collection of two or more sub-tasks. Once a Combined Task is created, device lists have to be associated with each sub-task of the Combined Task.

**Note:** Only device lists can be associated with the sub-tasks of the combined task. Individual devices cannot be associated.

### To execute a Combined Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the Combined Task to be executed on the **Batch Configuration** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed. The **Sub-Task List** table lists the sub-tasks under various protocols.
4. Clicking a protocol displays the Device List information on the **Device Lists for <Protocol>**. Select the device list that needs to be associated with the sub-task.
5. Click **Finish** to start the configuration.

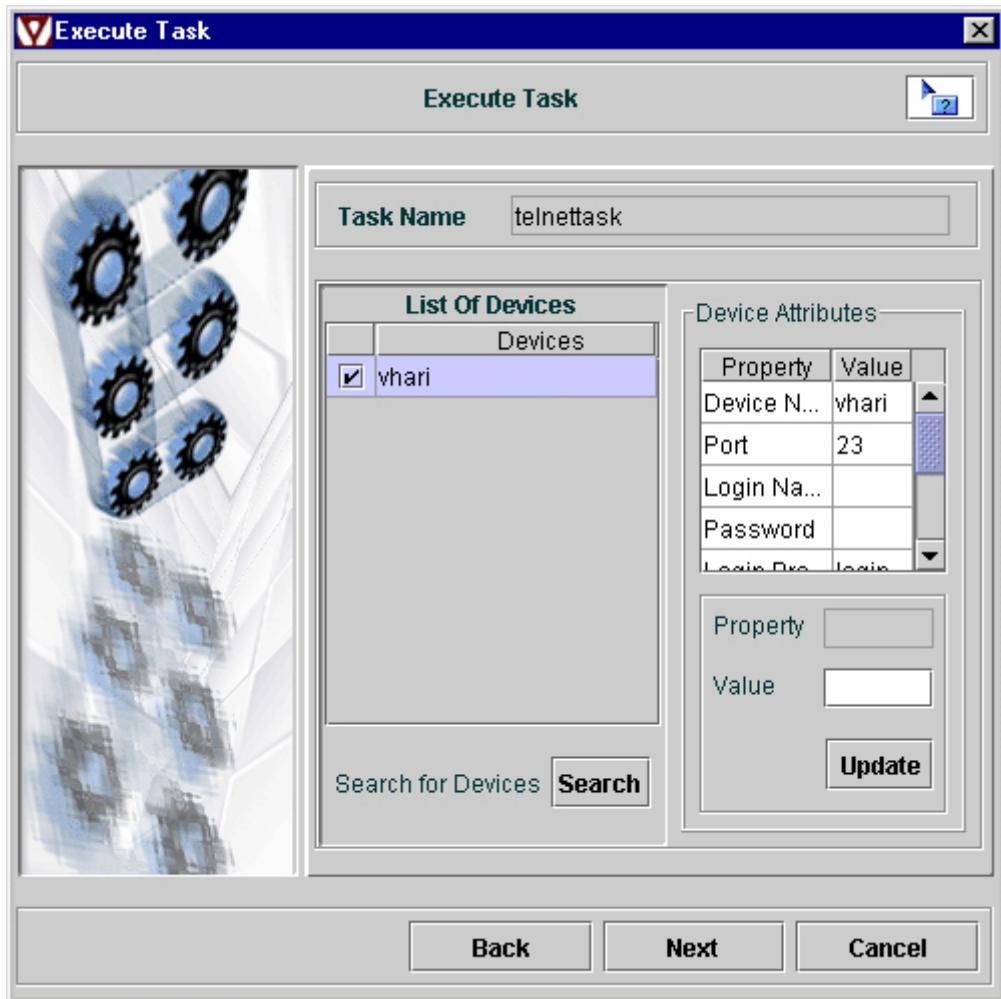
Once the task is executed, the time of execution is updated in the **Batch Configuration** panel. You can view the task audit details to know the attributes that have been configured.

## Executing Telnet Tasks

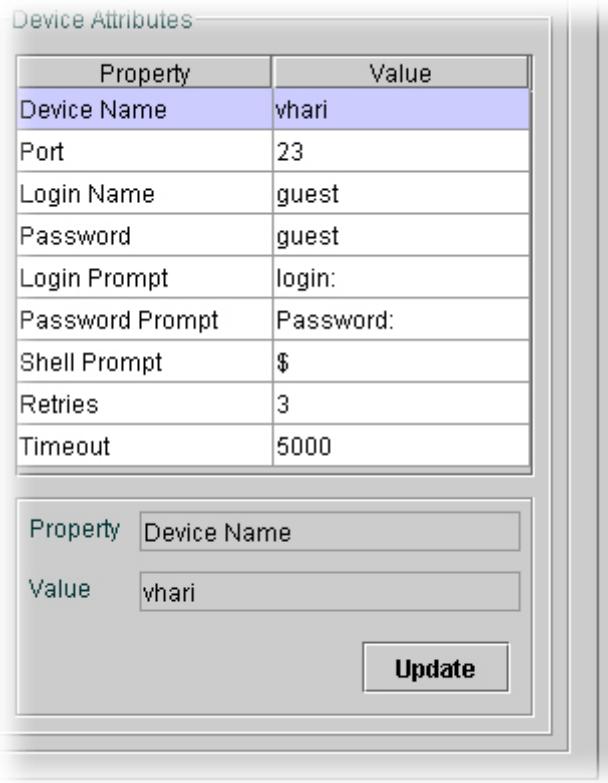
The procedure to execute a Telnet Task differs from that of the ordinary Tasks.

### To execute a Telnet Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the Telnet Task to be executed on the **Batch Configuration** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. Select **Would you like to associate devices for this task** to associate devices with the Task.



5. Click **Next**.
6. Use the **Search** option to locate the device to be configured. If found, the device is displayed in the **List of Devices** table. The device information is displayed in the **Device Attributes** table. Select the device. To change the value of any attribute, select the attribute, specify the new value in the **Value** field, and click **Update**. Values for the following attributes need to be specified.



- **Login Name:** The login name used for connecting to the device.
- **Password:** The password for the login name to connect the device.
- **Login Prompt:** The login prompt shown by the machine when the user logs in.
- **Password Prompt:** The password prompt shown by the machine when the login name is specified.
- **Shell Prompt:** The prompt that the machine displays after logging into the system.
- **Retries:** The number of retries to be performed for configuring the device.
- **Timeout:** The timeout value for each retry done. **Tip:** Some device may take a longer time to show the login and password prompt. Hence, it is recommended to provide longer timeout values.

6. Click **Next**. The devices available for the task execution are displayed.
7. Click **Finish** to start the configuration.

Once the task is executed, the time of execution is updated in the **Batch Configuration** panel. You can view the task audit details to know the attributes that have been configured.

## Uploading Configuration from Devices

Uploading Configuration from a device denotes fetching of values of the attributes from a device. To upload the configuration, a task has to be created. In this task, the attributes from which the data has to be fetched are defined.

**To upload configuration information from a device**

1. In the Web NMS Client, click **Configuration > Batch Configuration**.
2. Click the Task for which the attributes are to be updated from a device on the **Batch Configuration** panel.
3. From the **Config Operations** menu, choose **Upload Task** or press **Ctrl+U**. The **Task Upload** dialog box is displayed.
4. Specify the device name from which the configuration details need to be fetched and click **Add**. You can also locate the device using the **Search** option. The device is added to the list and its properties are displayed in the **Device Attributes** table.

**Note:** Although many devices can be added to the **Devices** list, upload can be done only from one device. Hence select the device on the list.

5. To edit the value of a device attribute, click the attribute, specify its value in the **Value** field, and click **Update**.
6. Click **OK**.

The device is configured with the Task and the values for the attributes present in the device are updated in the task. Once the upload is finished, the status of the operation is displayed. The upload fails for reasons, such as the agent not available, the agent not reachable, no such OID exists, and network congestion.

To confirm if the uploading has been successful, in the **Batch Configuration** panel, right-click the task and click **Task Details** or press **Ctrl+Shift+D**. The **Task Details** window is displayed. The **Value** field displays the value fetched from the device.

## 6.6.5 Executing Default Tasks

A set of default Tasks have been provided with Web NMS Configuration Management which can be used to configure devices, such as Switches, Routers, etc. These default tasks can also be considered examples provided to leverage the benefits provided by the module.

This topic explains the purpose and the procedure to execute the following default Tasks.

- 
- AcmeCardConfiguration
  - BroadCastStormControl
  - CiscoAccessListGeneration
  - CiscoAccessListDeletion
  - CiscoConfigBackup
  - FileTransfer
  - NATAddition
  - NATRemoval
  - NetworkDiscovery
  - RouteAdd
  - RouteDelete
  - SystemDateConfiguration
  - SystemGroupConfiguration
  - TrapForwarder

---

### AcmeCardConfiguration

**Purpose:** This task changes the **PRIORITY** value to **2** for the property **messagePayLoadBlock** for AcmeTL1Concentrator. Inputs like **TL1 command** (to change the properties of the card), and **AccessID** (to represent ST1 card present in the 5th slot) are provided, by default.

**Protocol:** TL1

#### To execute AcmeCardConfiguration Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **AcmeCardConfiguration** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. If a Device List already exists, it is displayed in this screen. Select the Device List. If you need to associate more devices for this task, select the **Would you like to associate more devices for this task** option.
5. Click **Next**.
6. All attributes and values of the devices are displayed. To change any values of attributes, select the attribute, edit its value in the **Value** field and click **Update**.
7. Click **Finish**.

## BroadCastStormControl

**Purpose:** This task configures the Broadcast threshold value for Cisco Systems Catalyst 1900 switches and generates traps which can be sent to any Trap Manager. The Trap generated is the trapBroadcastStorm (ST - 6 and GT 4)". This task accepts inputs, such as **Trap community**, **Trap manager name**, and **Broadcast threshold**.

**Protocol:** Telnet

### To execute BroadCastStormControl Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **BroadCastStormControl** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. From **Available Data Sources**, select **broadcastdatasource**.
5. Click **Configure Data Source Parameters**. The **Configure Data Source Parameters** dialog box is displayed.
6. Provide values for the keys. Select the key in the table, specify the value in the **Value** field and click **Update**.
  - **community**: Specify the trap community string (public or private).
  - **thresholdValue**: Specify the value that acts as a threshold.
  - **snmpManager**: Specify the IP address to which the traps are to be forwarded.
7. Click **OK**.
8. Click **Next**.
9. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## CiscoAccessListGeneration

**Purpose:** This task is used to add an **access list** to Cisco C2600 series router. Access lists are useful for preventing the access from or to the router for a number of services. This task adds an access list to enable permission for Telnet service for two IP addresses. This task requires inputs, such as **Access-list value**, **IP Address 1**, and **IP Address 2**.

**Protocol:** Telnet

### To execute CiscoAccessListGeneration Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **CiscoAccessListGeneration** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. From **Available Data Sources**, select **accesslistgenerationdatasource**.
5. Click **Configure Data Source Parameters**. The **Configure Data Source Parameters** dialog box is displayed.
6. Provide values for the keys. Select the key in the table, specify the value in the **Value** field, and click **Update**.
  - **Password**: Specify the password for adding the access list.

- acclistvalue: Specify a value between 0 to 99 (IP standard access list).
- IPAddress1: Specify an IP address for which access for telnet service has to be provided.
- IPAddress2: Specify another IP address to provide access for telnet service.

7. Click **OK**.
8. Click **Next**.
9. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## CiscoAccessListDeletion

**Purpose:** This task is used to delete the access list already created in the Cisco C2600 series router. Refer to the CiscoAccessListGeneration task. This task accepts the **Access-list value** and accordingly removes the permissions to access the device.

**Protocol:** Telnet

### To execute CiscoAccessListDeletion Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **CiscoAccessListDeletion** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. From **Available Data Sources**, select **accesslistdeletiondatasource**.
5. Click **Configure Data Source Parameters**. The **Configure Data Source Parameters** dialog box is displayed.
6. Provide values for the keys. Select the key in the table, specify the value in the **Value** field, and click **Update**.
  - Password: Specify the password for configuring the router.
  - acclistvalue: Specify the access list value that has to be deleted from the router.
7. Click **OK**.
8. Click **Next**.
9. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## CiscoConfigBackup

**Purpose:** This task is used to take a backup of the configuration information of a router. The backup information is stored in a file and transferred to a destination machine, where TFTP service is running. This task requires the following inputs: **IP Address** of the machine from where configuration information is to be read and **name of the file** in which the information is to be stored.

**Protocol:** Telnet

### To execute CiscoConfigBackup Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **CiscoConfigBackup** Task on the **Batch Execution** panel.

3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. From **Available Data Sources**, select **backupdatasource**.
5. Click **Configure Data Source Parameters**. The **Configure Data Source Parameters** dialog box is displayed.
6. Provide values for the keys. Select the key in the table, specify the value in the **Value** field, and click **Update**.
  - Password: Specify the password for configuring the router.
  - fileName: Specify a valid filename to which the configuration information of the router is to be copied.
  - IPAddr: Specify an IP address to which the configuration file is transferred. Make sure that the TFTP service is running in the host.
7. Click **OK**.
8. Click **Next**.
9. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## FileTransfer

**Purpose:** This task is used to transfer files between two machines. This task, by default, transfers the **README.html** file to a remote Host.

**Protocol:** TFTP

### To execute FileTransfer Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **FileTransfer** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## NATAddition

**Purpose:** This task adds an entry in the **Network Address Translation (NAT)** table and is specific to Cisco C2600 series. This will allow hosts with private IP Addresses to access the Internet. The **private IP addresses** and the **Access list** permissions are to be given as inputs.

**Protocol:** Telnet

### To execute NATAddition Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **NATAddition** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. From **Available Data Sources**, select **nataadddatasource**.

5. Click **Configure Data Source Parameters**. The **Configure Data Source Parameters** dialog box is displayed.
6. Provide values for the keys. Select the key in the table, specify the value in the **Value** field and click **Update**.
  - Password: Specify the password for configuring the router.
  - incomingInterface: Specify the name of the interface that acts as an incoming interface.
  - outgoingInterface: Specify the name of the interface that acts as an outgoing interface.
  - listno: Specify a number between 0 and 99 (IP Standard access list).
  - IPAddress1: Specify an IP address for which access list needs to be added.
  - IPAddress2: Specify an IP address for which access list needs to be added.
7. Click **OK**.
8. Click **Next**.
9. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## NATRemoval

**Purpose:** This task deletes the entry from the **Network Address Translation (NAT)** table, thus preventing the private IP address to browse through the Internet. This task is specific to Cisco C2600 series. Refer to the NATAddition section to learn how to add the IP addresses.

**Protocol:** Telnet

### To execute NATRemoval Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **NATRemoval** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. From **Available Data Sources**, select **natdeletedatasource**.
5. Click **Configure Data Source Parameters**. The **Configure Data Source Parameters** dialog box is displayed.
6. Provide values for the keys. Select the key in the table, specify the value in the **Value** field, and click **Update**.
  - Password: Specify the password for configuring the router.
  - incomingInterface: Specify the name of the interface that acted as an incoming interface.
  - outgoingInterface: Specify the name of the interface that acted as an outgoing interface.
  - listno: Specify a number between 0 and 99 (IP Standard access list).
7. Click **OK**.
8. Click **Next**.
9. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## NetworkDiscovery

**Purpose:** This task is useful to dynamically add a row to the **networkDiscoveryTable** of AdventNet-WebNMS-MIB. This will enable you to configure the networks to be discovered dynamically. Inputs, such as netIPAddress, EndIPAddress, netMask, StartIPAddress, and networkDiscoveryIndex are to be given.

**Protocol:** SNMP

### To execute NetworkDiscovery Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **NetworkDiscovery** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. From **Available Data Sources**, select **networkdiscoverydatasource**.
5. Click **Configure Data Source Parameters**. The **Configure Data Source Parameters** dialog box is displayed.
6. Provide values for the keys. Select the key in the table, specify the value in the **Value** field and click **Update**.
  - **netIPAddress**: Specify the IP address of the network to be discovered.
  - **EndIPAddress**: Specify the ending IP address until which the elements are to be discovered.
  - **netMask**: Specify the netmask value to find out the class to which the network belongs.
  - **StartIPAddress**: Specify the starting IP address from which the elements are to be discovered.
  - **networkDiscoveryIndex**: Specify a valid integer value for this field that will act as index value to the table.
7. Click **OK**.
8. Click **Next**.
9. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

Once the configuration is done, you can see that the network being discovered automatically based on the inputs provided and an entry will be added to the Client tree.

## RouteAdd

**Purpose:** This task adds an IP route for the information packets sent from a network. It helps in redirecting the packets to a particular interface within the router, so that the packets reach their desired destination.

**Protocol:** Telnet

### To execute RouteAdd Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **RouteAdd** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.

4. From **Available Data Sources**, select **routeadddatasource**.
5. Click **Configure Data Source Parameters**. The **Configure Data Source Parameters** dialog box is displayed.
6. Provide values for the keys. Select the key in the table, specify the value in the **Value** field, and click **Update**.
  - Password: Specify the password for configuring the router.
  - network: Specify the name of the network for which IP route has to be added.
  - mask: Specify the mask for determining the class to which the network belongs.
  - Interface: Specify the name of the interface to which the packets have to be redirected.
7. Click **OK**.
8. Click **Next**.
9. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## RouteDelete

**Purpose:** This task deletes an IP route, thus hindering the flow of information packets sent from a network.

**Protocol:** Telnet

### To execute RouteDelete Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **RouteDelete** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. From **Available Data Sources**, select **RouteDelete**.
5. Click **Configure Data Source Parameters**. The **Configure Data Source Parameters** dialog box is displayed.
6. Provide values for the keys. Select the key in the table, specify the value in the **Value** field, and click **Update**.
  - Password: Specify the password for configuring the router.
  - network: Specify the name of the network, whose IP route has to be deleted.
  - NetMask: Specify the mask for determining the class to which the network belongs.
7. Click **OK**.
8. Click **Next**.
9. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## SystemDateConfiguration

**Purpose:** This task is used to configure the system date and time of a TL1 machine. On executing this task, the system date is set to **2001-12-27** and time is set to **11 hours 11 minutes** and **11 seconds**.

**Protocol:** TL1

### To execute SystemDateConfiguration Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **SystemDateConfiguration** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## SystemGroupConfiguration

**Purpose:** This task is used for configuring the SNMP attributes of a remote host. The system variables **1.5.0** (sysName) and **1.6.0** (sysLocation) are set to **test1** and **test2** respectively.

**Protocol:** SNMP

### To execute SystemGroupConfiguration Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **SystemGroupConfiguration** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

## TrapForwarder

**Purpose:** This task forwards all the traps that are received in a specific port of one machine to the destination port of another machine by adding a row to the **Forwarding** table of AdventNet-WebNMS-MIB. The destination host name and its port to which the traps need to be forwarded are given as input.

**Protocol:** SNMP

### To execute TrapForwarder Task

1. In the Web NMS Client, click **Configuration > Batch Configuration**. All the existing Tasks are displayed on the right-side **Batch Configuration** panel.
2. Click the **TrapForwarder** Task on the **Batch Execution** panel.
3. From the **Config Operations** menu, choose **Execute** or press **Ctrl+E**. The **Execute Task** wizard is displayed.
4. From **Available Data Sources**, select **trapforwarderdatasource**.
5. Click **Configure Data Source Parameters**. The **Configure Data Source Parameters** dialog box is displayed.
6. Provide values for the keys. Select the key in the table, specify the value in the **Value** field, and click **Update**.
  - **managerHost:** Specify the destination host where the traps are to be forwarded.
  - **ID:** Any valid integer. This acts as an index entry in the TrapForwarding table.

- rowStatus: Specify the rowStatus as **4**. This corresponds to the **createAndGo** option.
- managerPort: Specify the port in the destination host, where the trap are to be forwarded.

7. Click **OK**.
8. Click **Next**.
9. Follow steps 4 to 7 as explained in the To execute AcmeCardConfiguration Task section.

You can view the traps received by Web NMS application being forwarded to the specified *managerHost* at the specified port, using the Trap Viewer.

## 6.6.6 Auditing

**Auditing** is a functionality by which all the configuration changes done to the device are stored in the Configuration Server to perform auditing. An **Audit** provides administrators with details, such as name, starting time, finishing time, status (success or failed) of the configuration, etc.

- Viewing Audits
- Viewing Attribute-Level Audit Details
- Working with Custom Views
- Searching Audit Details

### Viewing Audits

#### To view audits

- In the Web NMS Client, click **Configuration > Audit**. The Audit panel is displayed on the right-side panel which lists all the audits. By default, the details of **Task Name**, **Device Name**, **Start Time**, **Finish Time**, and **Status** are displayed.

### Viewing Attribute-Level Audit Details

The Attribute-Level Audit helps you to know the status of the configuration of each attribute.

#### To view Attribute-Level Audit Details

1. In the Web NMS Client, click **Configuration > Audit**. Existing Audits are displayed on the right-side **Audit** panel.
2. Select the Audit for which you need to view the attribute details.
3. From the **View** menu, choose **Attribute Audit** or press **Ctrl+A** or right-click the Audit and choose **Attribute Audit**. The **Attribute Audit Details** window is displayed with the following attribute details:
  - **Attribute Name:** Name of the attribute that was configured on the device.
  - **Finish Time:** Time at which the attribute was configured.
  - **Retries:** Number of retries after which the attribute was configured successfully.
  - **Status:** Status of the attributes after configuration.

### Working with Custom Views

Custom Views are user-defined views that satisfy certain match criteria. The Custom Views can be used to limit the information presented to the user. This section explains:

- Adding Custom View
- Modifying Custom View
- Saving Custom View
- Renaming Custom View
- Deleting Custom View

## Adding Custom View

### To add a custom view

1. In the Web NMS Client, click **Configuration > Audit**.
2. From the **Custom Views** menu, choose **Add Custom View** or press **Ctrl+V**. The **Add Custom View Form** dialog box is displayed.
3. Specify appropriate values in the following fields and click **Next**.

Field	Description
Custom View Name	Specify name for the custom view you are creating or modifying.
Parent Node	Choose the parent tree node under which your custom view has to be placed in the tree, from the drop-down box.  The criteria set for the parent custom view will be automatically used for child custom view. Hence, it is enough to specify only additional criteria for the child custom view.
Frame Title	Specify the name to be displayed on the title bar of the custom view.
Icon File Name	Specify the icon name (in the <i>&lt;Web Home&gt;/images</i> directory) to use for the custom view. This icon is visible in the tree as well as in the title bar of the custom view.
Menu File Name	Specify the panel-specific menu filename. If no value is specified, the default menu is displayed.
Table Popup Menu	Specify the filename of the menu used to display a contextual menu for the Audits displayed in the table of the new custom view.
Tree Popup Menu	Specify the file name of the menu used to display a contextual menu for the new custom view node in the Navigation tree.
Node Index	Specify the position (order of placement) of the custom view in relation to previously added views. If no value is specified, the view will be appended to the current list of custom views.

4. In the next screen, specify the criteria based on which you need data to be displayed in your custom view. For example if you specify **Task Name**, **starts with**, and **test** in **Property**, **Operation**, and **Value** fields respectively, only Tasks starting with **test** are displayed in your custom view.

To specify more than one criterion, click **More**. Additional fields are available. After specifying the criteria, click **Next**.

5. The next screen displays all the properties that are displayed as columns in the Audit panel. By default, the **Audit** panel displays **Task Name**, **Device Name**, **Start Time**, **Finish Time**, and **Status** as its columns. If you need more properties to be displayed, select the check boxes of the properties. As you select, a preview of the columns is displayed below the fields.
6. On specifying necessary values, click **Finish**.

A new tree node with the newly added custom view name is created and the custom view can be accessed by clicking on that node.

## Modifying Custom View

### To modify a custom view

1. In the **Audit** panel, click the custom view on the tree.
2. From the **Custom Views** menu, choose **Modify Custom View** or press **Ctrl+M** or right-click the custom view tree node and choose **Custom Views > Modify Custom View**. The **Modify Custom View Form** dialog box is displayed.
3. Make appropriate modifications and click **Finish** in the final screen. For information on each of the fields, refer to the Adding Custom View procedure.

## Saving Custom View

### To save a custom view

1. In the **Audit** panel, click the custom view on the tree.
2. From the **Custom Views** menu, choose **Save Custom View State** or press **Ctrl+S** or right-click the custom view tree node and choose **Custom Views > Save Custom View State**. Once the custom view is saved, a message confirming the same is displayed in the status bar.

On performing this, the sorting and the column width in the custom view is saved in the Server; and each time the Client is restarted, the custom views are fetched from the Server for display.

## Renaming Custom View

### To rename a custom view

1. In the **Audit** panel, click the custom view on the tree.
2. From the **Custom Views** menu, choose **Rename Custom View** or press **F2** or right-click the custom view tree node and choose **Custom Views > Rename Custom View**. The tree node is editable.
3. Specify the new custom view name and press **Enter**.

## Deleting a Custom View

### To delete a custom view

1. In the **Audit** panel, click the custom view on the tree.
2. From the **Custom Views** menu, choose **Remove Custom View** or press **Ctrl+C** or right-click the custom view tree node and choose **Custom Views > Remove Custom View**. A confirmation is asked.
3. Click **Yes** to delete the custom view.

## Searching Audit Details

The Audit panels display all the Audits of configuration task performed. When there are more number of Audits displayed, use the **Search** option to locate a specific Audit.

### To search audit details

1. In the Web NMS Client, click **Configuration > Audit**. Existing Audits are displayed on the right-side **Audit** panel.
2. From the **Edit** menu, choose **Search** or press **Ctrl+F**. The **Search** dialog box is displayed.
3. If you want to perform a search operation that satisfies any of the matching criteria that you specify, select **Match any of the following**. If you need all the matching criteria to be satisfied for your search operation, select **Match all of the following**.
4. In the **Properties** field, select the property based on which you need to perform your search.
5. In the **Conditions** field, select the condition based on which you need to restrict your search.
6. In the **Value** text field, enter the exact information you are looking for. If you have selected time-related properties in the **Property** field, a Time spin box is displayed wherein you need to set the date and time.
7. To specify additional criteria, click **More** and add more criteria. The **Fewer** option can be used to remove the criteria that were last added.
8. To begin the search, click **Search**.

## 6.6.7 Configurable Parameters

The startup options of the Configuration Management module can be modified by editing the parameters of the **NmsConfigurationServer** process in the **NmsProcessesBE.conf** file located in the <Web NMS Home>/conf directory.



**Note:** If you have configured any of the parameters, ensure to restart the Web NMS Server.

The parameters that can be configured by administrators after deployment are listed below. For complete information, follow the links provided for each of the parameters.

- To change the ConfigServer port - CONFIG\_SERVER\_PORT
- To enable the Debug option - DEBUG
- To change the level of debugging - DEBUG\_LEVEL
- To control the audit levels - AUDIT\_LEVEL
- To control the number of audit records - CLEAN\_AUDIT\_INTERVAL

## 6.7 Performance Management

In the Web Client, choose **Performance > Configured Collection** to view the performance data of network elements.

The following are the administrative operations that you can perform from this view.

---

- Getting Started
  - Configuring Data Collection
  - Adding Statistics at Runtime
  - Defining Thresholds
  - Clearing the Data
  - Setting User Privileges
  - Configurable Parameters
-

## 6.7.1 Performance Management: Getting Started

This topic helps you get started with the Performance Management module of Web NMS. Some of the performance-related concepts are discussed here.

The main input to performance module is the Managed objects created to represent network devices. These Managed objects are created by Web NMS Topology module when discovery process takes place. Managed Objects hold details of the network element such as Name, Type, status, etc. Data collection is configured for these Managed objects in the Performance module.



**Note:** By default, Managed objects are created by Web NMS Topology module and added into database. If you do not want to use Web NMS Topology module for discovery then you have to take care of creating Managed objects and adding them into database. Performance module acts as an observer to Topology module. When Managed objects are added to database notification will be received by Performance module. Hence, ensure that Managed objects are added to Web NMS database using TopoAPI.

Performance Management deals with two main functions:

- Data Collection
- Threshold Application

### Data Collection

Network performance is evaluated based on how each network element is performing. To evaluate, data has to be collected from those elements. Each device deals with varied data, some of them being

- How many octects (bytes) it receives
- How many octects (bytes) it sends
- What is the speed of the device in responding and lot more.

Hence, you must know from which device to collect data and what data to collect.

**Related Topic:** Configuring Data Collection

### Threshold Application

Once data collection starts, it is stored in the database for future reference. To monitor network performance, you need to check if the collected data is optimal. For example, the optimal speed of switch Rk5 should be 100000 to be considered efficient.

Hence, to perform such checks, you need to define **Thresholds**. A Threshold object contains a value as the maximum or minimum limit for the collected data. If the collected data from the device exceeds this limit, it means the device performance is degrading.

Hence, you need to understand how to create Thresholds and associate them with the data to be monitored.

Apart from these two main functions, you also need some means to view the results of Data collection and Threshold Application. For this purpose, the Web NMS Performance module provides you a Notification and Reporting mechanism.

**Related Topic:** Defining Thresholds

## 6.7.2 Configuring Data Collection

Data collection is the process of collecting useful information from network elements, such as computers, switches, routers, etc. The collected data is used in formulas which calculate network performance. The performance of your network depends on the data you select. This section explains the pattern - **what data to collect, from which device, and in what manner**.

- Purpose
- Elements Involved in Data Collection
- Data Collection Process

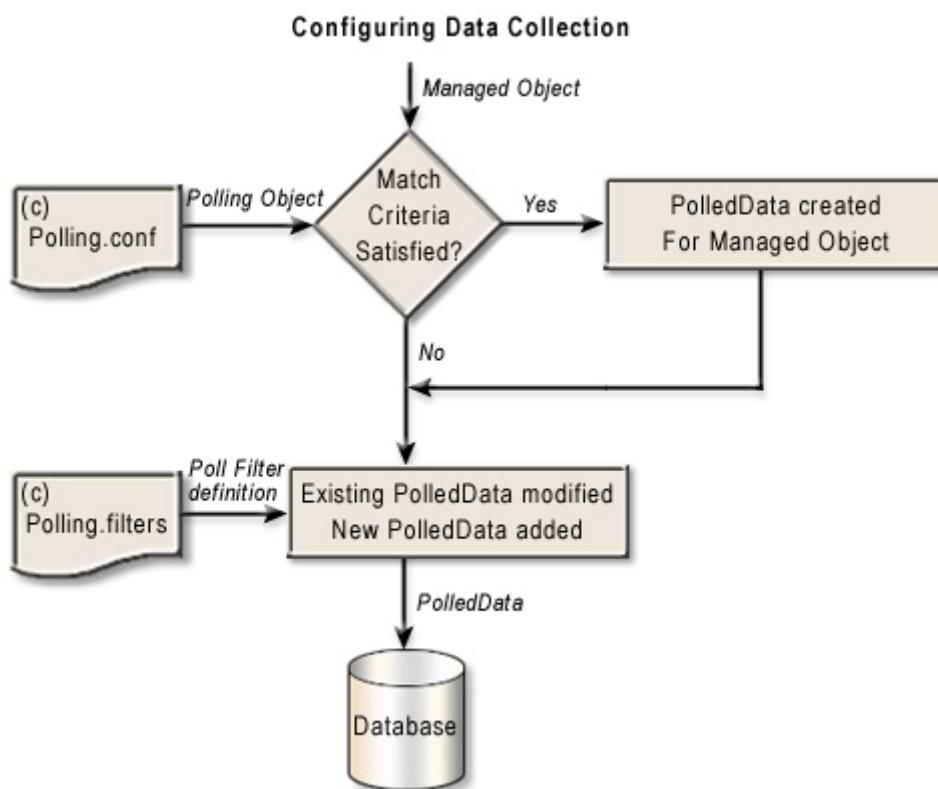
### Purpose

By Configuring Data Collection, you can

1. specify from which devices the data is to be collected.
2. choose particular data to be collected or not.
3. temporarily stop data collection and resume whenever wanted.
4. choose protocol of your choice for data collection.
5. set storage options and specify when and where to store data.

### Elements Involved in Data Collection

To configure data collection in Web NMS, an understanding of the process carried out and the various elements involved in the process is required.



## Elements

### Managed Object (MO)

This object is created by Topology module. An MO represents an entity which can be a device (as a whole) or a part of the device (port, card, slot, interface). An MO contains the properties of the entity, such as name, and type.

For example, assume the MO to be a port in Windows NT machine and name of the machine to be **WinNT1**. Then the MO has the properties: Name = WinNT1 & Type = Port

### Polling Object

This object is created by Performance module. This object contains the following two properties:

- **Match Criteria** denotes the conditions to be satisfied by the MO. Only when these conditions are satisfied will MO be considered for data collection. For example, isSNMP = true. This Match Criteria denotes that the MO should be an SNMP node.
- **Data Collection Criteria** denotes the list of data to be collected from the MO.

### PolledData

This is the unit of data collection, i.e., when you specify what data to be collected in Polling Object, a PolledData is created for each of the definition of what data to be collected and using this PolledData, data is collected and stored in the database.

For example, if the data *number of octets received by the interface of a device* has to be retrieved then a PolledData with name *Interface\_if\_inoctet* can be created.



**Note:** PolledData is also called **Statistics**. Hence, in the User interface forms and menu options, you will see PolledData objects referred to as **Statistics**.

PolledData can be created either **via Polling object** definition or **directly** for a Managed object.

### Using PollingObject

- The value set for status property of PollingObject will reflect upon the PolledData.
- The set of PolledData will be treated as a single group and deletion of PollingObject will automatically delete the associated PolledData.
- It is useful when you want to create many PolledData for individual ManagedObjects wherein the PollingObject's match criteria will satisfy the ManagedObject properties.

### Directly

- Only one PolledData can be added at a time for a ManagedObject and each has to be handled i.e. modified and deleted individually.
- Suitable when less number of PolledData are to be created.
- PolledData added for the same ManagedObject i.e. using PollingObject and directly, is treated separate. Any change in the PollingObject associated with the ManagedObject will not affect the PolledData added directly to the ManagedObject.

## Poll Filter

When PolledData is created for an MO as specified in data collection criteria, it can undergo a change in properties or some more PolledData can be added or existing set may need to be deleted. This is achieved by creating a Poll Filter object in which the action to be performed is defined.

## Configuration Files

Following are the two performance-related configuration files.

- **Polling.conf:** This contains the definition of Polling objects. This definition is read during Server startup. Polling Objects are created based on this definition and stored in database.
- **Polling.filters:** This contains name of the Poll Filter class.

## Data Collection Process

These are the steps involved in configuring data collection:

1. At Server startup, Polling Objects are created based on the definition present in **Polling.conf**. Each Polling object in itself contains two definitions: **Match criteria** and **Data collection criteria**.
2. Whenever a Managed Object is created by Topology module, it is given as input to the Polling Object.
3. The Polling object's Match criteria is compared with Managed Object's properties.
4. If Match criteria is met, PolledData is created for every entry specified in Data collection criteria.
5. If there exists Poll Filters, then the created PolledData is passed through the Poll Filter one by one to undergo appropriate modifications. Then the filtered PolledData is added to the database.
6. If Poll Filters does not exist then PolledData is added to the database as it is.
7. Even if the Match criteria is not satisfied, the Managed object is passed through Poll Filters. Because, if you want to add a single PolledData for a particular Managed object, you need not create a Polling object. Polling object creation is best suited when you want to add a large set of PolledData for a Managed object.

Thus, the definition of **what data to collect** and **from which device** is recorded in the database, and Performance module uses this information for data collection.

## 6.7.2.1 Selecting Devices for Data Collection

This topic explains how to create Polling Objects, using an example. This can be achieved by using a User Interface from the Web NMS Client.

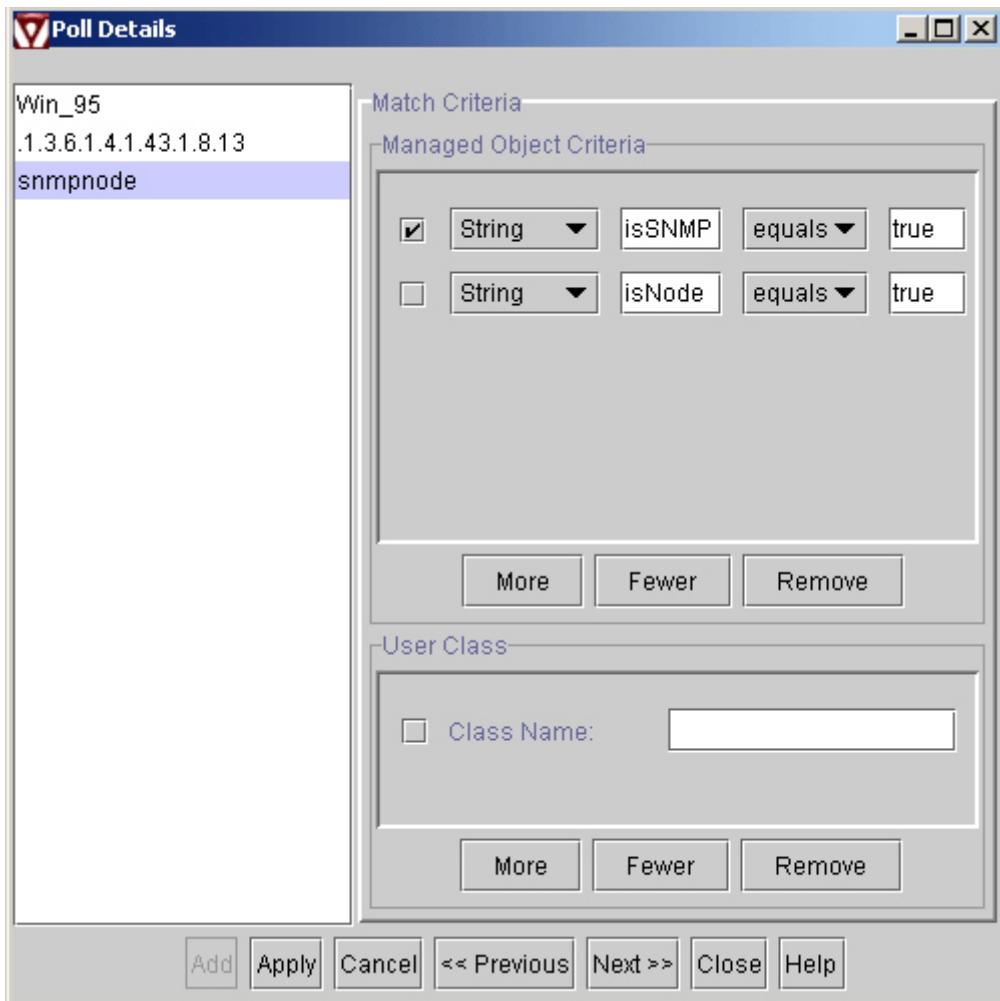
Let us assume that you want to create a Polling Object to identify Managed Objects (MO) which follow SNMP and are of type **Node**. Type of the MO denotes whether it is a node, network, router, switch, etc.

### To create a Polling Object

1. In the Web NMS Client, choose **Performance > Configured Collection**.
2. From the **Edit** menu, choose **Polling Objects > Add Polling Objects**. The **Poll Details** wizard is displayed.
3. Click **Add**. Specify appropriate values in the following fields (each field is a property of the Polling Object).
  - **Polling Object Name:** A string to identify the Polling object. Example: NodePollObj. This is a **mandatory** field.
  - **Status:** Available as check box. When selected (tick), it indicates true, otherwise false. When Polling object's status is set to true, it is active and data collection for its associated PolledData can be done. If set to false, data collection for the associated PolledData will be stopped. **Default value:** *true*
  - **Update Managed Objects:** Available as check box. When selected (tick), it indicates that the Polling Object's definition will be applied over existing Managed Objects and they will be updated with information given in Polling objects.

**Example:** Assume you have twenty MOs and for each you have two PolledData added. Suppose, if you want to add two more PolledData for a particular set of Managed Objects, you can specify the match criteria in Polling Object and the information regarding the new PolledData. Now if this field is selected, as soon as a Polling Object is added, for the existing MOs that satisfy the match criteria, the two PolledData will be added. If this option is not selected, the Polling Object will be used for newly created MO only. **Default value:** *false*

4. Click **Next**. The next screen of the wizard is to set the **Match Criteria** which a Managed Object should satisfy for data to be collected from it.



You can specify the Match criteria in two ways:

- Using Managed Object Properties
- Using User Class

#### **Using Managed Object Properties ( You have to specify at least one property )**

Each MO has a set of properties. You can use those properties in the Match criteria.

**Example:** One of the properties of an MO is **isSNMP**. This stores the value **true** if the MO denotes an SNMP object (i.e. which uses SNMP for communication). So you can specify one of the match criteria as **isSNMP = true**.

You can specify any number of match criteria. Only limitation is that Web NMS Performance module currently supports only comparing **String** and **Long** values.

#### **To specify a match criteria**

1. Choose the type of Property to be compared, i.e., String or Integer.
2. Specify the MO property.
3. Choose the comparison operator that has to be displayed based on the type you have chosen.
4. Specify the value to be compared.

For this example, set the following values:

String	isSNMP	equals	true
String	isNode	equals	true

The default set of MO properties are listed below. You can use these to set the match criteria. **Note:** Your environment can have some more properties added to MO and hence you must be aware of those new properties.

**status, type, managed, isGroup, isContainer, isSNMP, isDHCP, isRouter, isNode, isNetwork, isInterface, sysName, sysOID, ifSpeed, ifDescr, ifIndex etc**

**Tip:** There is a check box beside every Match Criteria row. To remove any match criteria row, select it and click Remove.

### Using User Class

When you specify a list of match criteria based on MO properties, an implicit AND operation is performed among the results i.e., if you specify 2 conditions, both of them have to be satisfied for the managed object to be considered for data collection. If you want to change this default pattern, you can write your own class and refer to it in **User Class** property. In your class, define the match criteria based on your requirement. **Example:** Specify that only if either of the 2 conditions satisfies, the MO for data collection should be considered.

A sample UserClass class file is available in the <Web NMS Home>/examples/performance management/userclass directory.

The next step is to define What data is to be collected from the device.

## 6.7.2.2 Defining the Data to be Collected

- 
- SNMP Data Collection
  - Choosing Data Identifier for Data Collection
  - Specifying Expressions using OIDs
- 

### SNMP Data Collection

Once it has been decided for which Managed Objects (MOs) data has to be collected, you have to choose the type of data to be collected and the location. Data from the MO can be accessed from its agent.

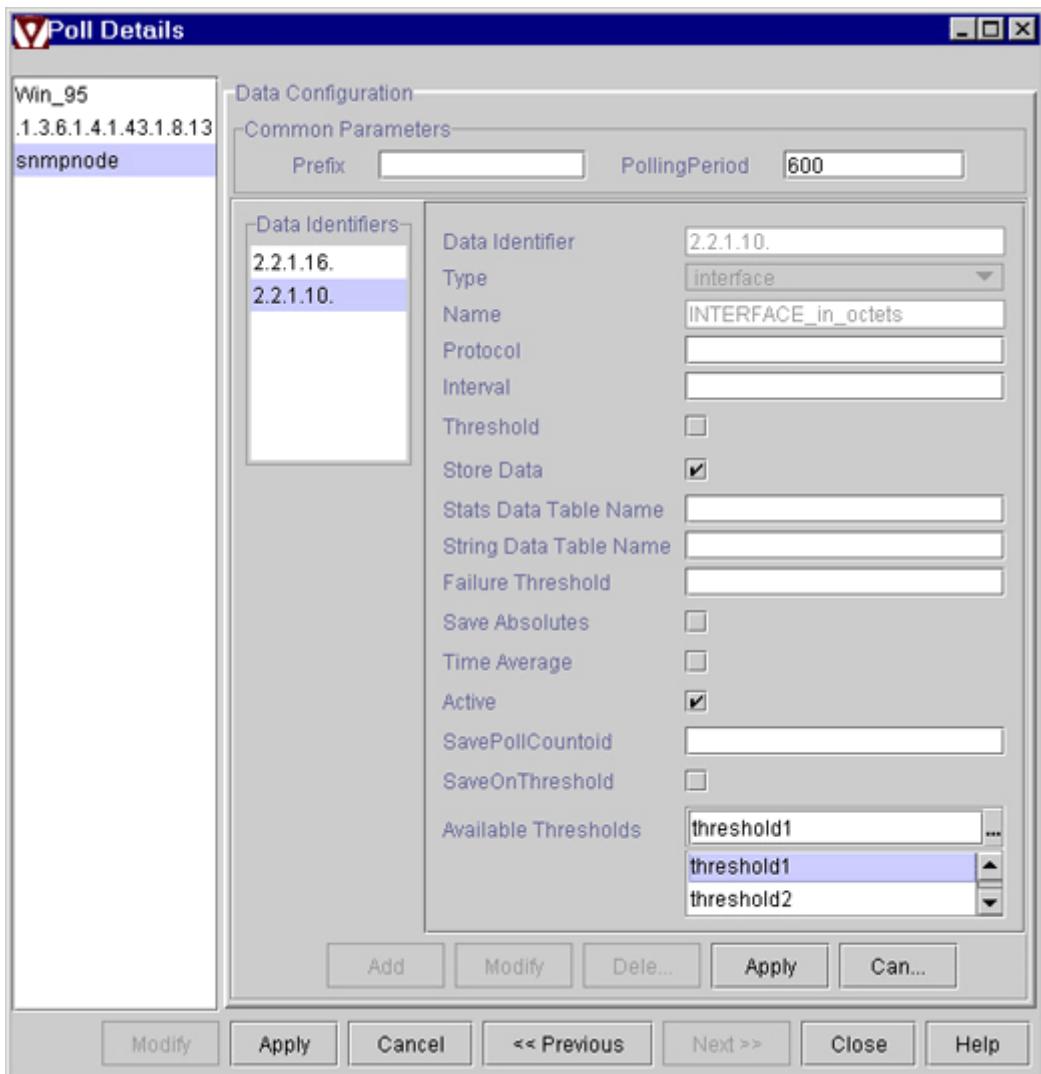
An **agent** is a program running in the device which awaits data collection request. When a request is made to the agent for a particular data, the corresponding OID (Object Identifier - A unique Identification number) has to be supplied. An **object identifier** uniquely identifies specific characteristic of the Managed object. Hence to collect the data you have to specify the OID for that characteristic. The term OID is generically used as **Data identifier**. OID is SNMP-specific term.

The list of Data Identifiers can be retrieved from the MIB definition of the device. **MIB** is a logical database made up of the configuration, status and statistical information stored in a device. Use the MIB Browser tool bundled with Web NMS product. Load the MIB of the device from which you want to collect data. Check out the Data Identifiers for which you want to collect data.

By default, Web NMS Performance module uses **SNMP** for data collection and **RFC1213 MIB Standards** for Data Identifiers. You can plug in your own protocol and choose Data Identifiers from different MIBs.

## Choosing the Data Identifier for Data Collection

In the Polling Object creation process, proceed to the third screen of the **Poll Details** dialog box, by clicking **Next**. For information on the procedure so far, refer to the Selecting Devices for Data Collection topic.

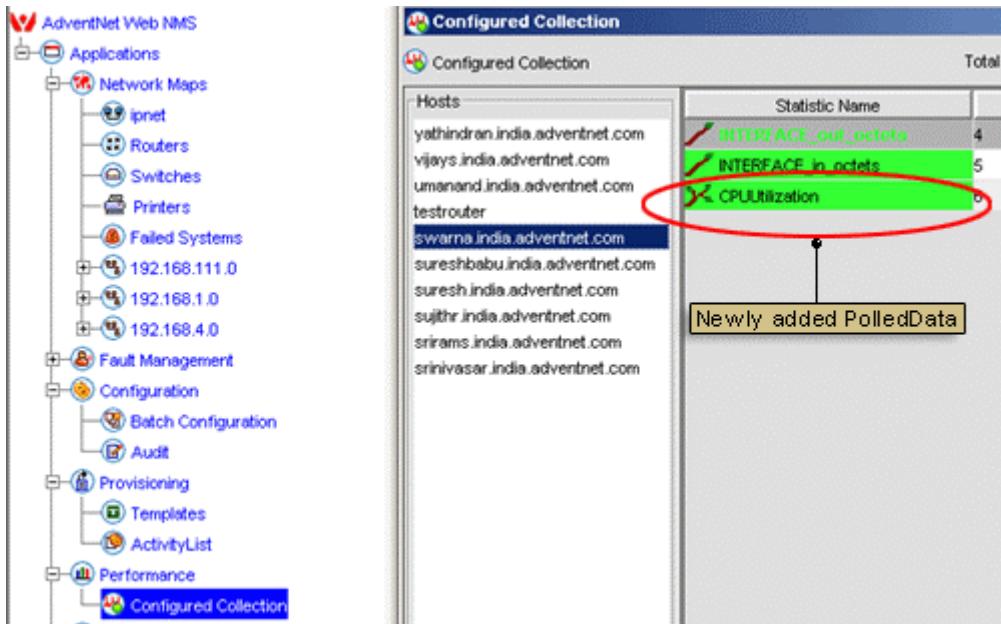


For information on the Common Properties and Data Identifier Properties, refer to Appendix.

For every Data identifier you add, click **Apply**. It is added to the **Data Identifiers** List box. To modify or delete any Data Identifier, select it from the list and click **Modify** or **Delete** respectively.

After you have added all the Data Identifiers, click **Apply** in the Polling Objects dialog box which adds the Polling Object definition to the database.

You can see the Data Identifier (Statistic) added in the **Configured Collection** panel for those hosts for which the match criteria have satisfied.



## Specifying Expressions using OIDs

You can form an expression using **Arithmetic operators** and **existing Data identifiers**.

**Example:** (.1.3.6.1.2.1.2.2.1.10.1 + .1.3.6.1.2.1.2.2.1.16.1) / 2

This means an average of data collected for the instances of IfInOctets and IfOutOctets Interface. You can specify expression OID in Conf file as well as in the UI. When you do so, data is collected for all the Data Identifiers involved in the expression and resultant value is calculated based on the expression.

### Note:

- You can create expressions only using Data Identifiers for which Long type data is collected. String OIDs cannot be used.
- Only the added value is stored in STATSDATA table and not the individual OID values.
- When you specify an Expression OID, specify the entire Data Identifier along with the prefix. Do not give prefix separately in the UI.
- Operators such as + (Addition), - (Subtraction), \* (Multiplication), / (Division), % (Remainder), &gt; (Right Shift), &lt; (Left Shift), : (Bitwise AND), | (Bitwise OR), ^ (Exclusive OR), min() and max can be used.
- min(oid 1, oid2), min(value1, value2) and max(oid1,min(oid2,oid3)) are valid expressions.
- Support available for specifying **\$DELTA\_TIME** as a replaceable parameter. **Example:** If you create a Polled Data with an expression OID, such as **(2.2.1.4.1 \* \$DELTA\_TIME)**, then the value collected for this expression will be the value retrieved for the OID 2.2.1.4.1 multiplied by the difference of the time between the current poll and previous poll of this poll data.

## 6.7.2.3 Managing Data Collection Configuration

- 
- Modifying Polling Object
  - Deleting Polling Object
- 

### Modifying Polling Object

You can

- Disable (or) deactivate the Polling Object. Doing so, data collection will stop for all the associated PolledData.
- Modify existing Data Identifiers associated with the Polling Object. You may require to modify some of their properties like Period of data collection, active state, threshold list, etc.
- Add new Data identifiers, i.e. PolledData to the Polling object.

#### To modify the Polling Object

1. In the Web NMS Client, choose **Performance > Configured Collection** on the tree.
2. From the **Edit** menu, choose **Polling Objects > Modify Polling Object**. The **Poll Details** wizard is displayed.
3. Choose the Polling Object (from the left pane) which you want to modify.
4. Click **Modify**.
5. In the right pane, modify the **Status**, if required.
6. **Update Managed Objects** is available as check box. When selected (tick), it indicates that the Polling Object's definition will be applied over existing Managed Objects and they will be updated with information given in Polling objects. For more information, refer to the Selecting Devices for Data Collection section.
7. Click **Next**.
8. You cannot edit the match criteria set for a Polling Object. This includes both **Managed Object Criteria** and **User Class** settings.
9. Click **Next**.
10. Select the Data Identifier to be modified from the **Data Identifiers** section and click **Modify**.
11. Make appropriate changes as required. For information on each of the fields, refer to the Defining What Data to Collect topic.
12. When the modifications are done, click **Apply** to apply the changes to the database.

### Deleting Polling Object

You can delete a Polling Object permanently from the system if you have decided not to perform data collection for certain devices any longer.

#### To delete a Polling Object

1. In the Web NMS Client, choose **Performance > Configured Collection** on the tree.
2. From the **Edit** menu, choose **Polling Objects > Delete Polling Object**. The **Poll Details** wizard is displayed.
3. Choose the Polling Object (from the left pane) which you want to delete.
4. Click **Delete**. A confirmation is asked.
5. Click **Yes** to delete the Polling Object.

On performing this procedure, the Polling Object and the Data Identifiers (Statistics) added via the Polling Object are removed from respective hosts.

## 6.7.3 Adding Statistics at Runtime

---

- Adding Statistics at Runtime
    - Modifying Existing Polling Object
    - Using 'Add Statistic' Option
  - Modifying Statistics
  - Deleting Statistics
  - Handling Extended PolledData
  - Active State of PolledData
- 

Before starting the Web NMS Server, you might have decided what data to collect and from which device. Accordingly, you might have configured Data collection by creating Polling Objects definition in **Polling.conf**. You might have also created Polling Objects at runtime using UI. Let's assume that you want to monitor extra information and you want the data to be collected for the device. In such a situation, you prefer adding a new **Statistic** to the system.



**Note:** The term PolledData and Statistic are used interchangeably. In the Client User interfaces, you will find the term Statistics used instead of PolledData and so do not get confused.

Assume you have added 3 PolledData via a Polling Object for all Windows 95 machines in your network. And also assume that now you have two requirements:

- To add another Statistic, say **IfInError** for all Windows 95 machine.
- To add a Statistic, say **SystemDescr** for one of the Windows 95 machine, i.e., **MACH3**.

To address these two requirements, you need to add the Statistic by one of these two methods:

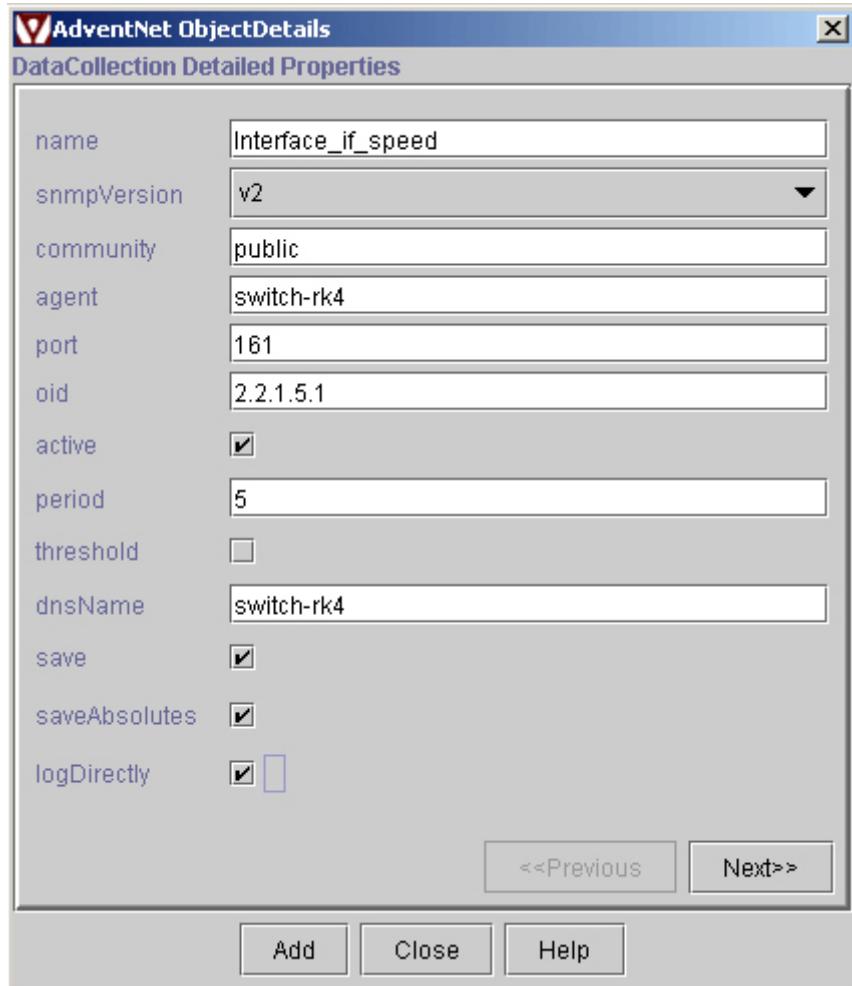
- Modifying existing Polling Object
- Using 'Add Statistics' Option

### Using 'Add Statistics' Option

When you need to add a Statistic for a few nodes, the best way is to use the **Add Statistics** option.

#### To add statistics at runtime

1. In Web NMS Client, choose **Performance > Configured Collection**.
2. From the **Edit** menu, choose **Add Statistics** or press **Ctrl+N**. The **Object Details** dialog box is displayed.



3. Specify appropriate values for the fields. Each of the fields in this screen is explained in Appendix.
4. Click **Next**.
5. Specify appropriate values in the fields. Each of the fields in this screen is explained in Appendix.
6. For additional properties, click **Additional Props**. The **PolledData Additional Properties** dialog box is displayed. Specify the property name and its value in the **Name** and **Value** field respectively. To add more user properties, click **More**. To remove a user property in this dialog box, select the property and click **Remove**. For fewer rows of properties, click **Fewer**. Click **OK**.

**Example:** **Name** = *Description* and **Value** = "This is an example Statistic"

7. Click **Add**.

In the **Configured Collection** panel, you can view the Statistic added for the device that you have just created.

## Modifying Statistics

### To modify an existing Statistic

1. In Web NMS Client, choose **Performance > Configured Collection**.
2. Select the Statistic in the **Configured Collection** panel.

3. From the **Edit** menu, choose **Modify Statistic** or press **Ctrl+Shift+M**. The **ObjectDetails** dialog box is displayed.
4. Make appropriate changes. For information on each of the fields, refer to Appendix. Some of the properties are non-editable as they are key factors in identifying the Statistic internally.
5. Click **Modify**.

The modifications to the Statistics are immediately applied and reflected.

## Deleting Existing Statistic

### To delete a Statistic

1. In Web NMS Client, choose **Performance > Configured Collection**.
2. Select the Statistic in the **Configured Collection** panel.
3. From the **Edit** menu, choose **Remove Statistic** or press **Ctrl+Shift+R**. A confirmation is asked.
4. Click **Yes** to delete the Statistic. User properties associated with the Statistics are automatically deleted.



**Warning:** If you wish to stop the data collection for a Statistic temporarily , it is not advisable to delete the Statistic. Instead, you can disable (uncheck) the **Active** property of the Statistic. Till you enable (check) it again, the data collection will not happen for the Statistic.

## Handling Extended PolledData

Web NMS facilitates creation of **Extended PolledData**, which contains the basic properties of a PolledData plus some extra properties defined specific to the client requirements. Extended PolledData creation is handled by the developer who customizes Web NMS for client usage.

As an Administrator, you can modify the values of those extra properties of the Extended PolledData object.

### To modify the properties of Extended PolledData

1. In Web NMS Client, choose **Performance > Configured Collection**.
2. Select the Statistic in the **Configured Collection** panel.
3. From the **Edit** menu, choose **Modify Statistic** or press **Ctrl+Shift+M**. The **ObjectDetails** dialog box is displayed.
4. Click **Additional Props** in the final screen. The **PolledData Additional Properties** dialog box is displayed. This dialog box displays the extra properties of the Extended PolledData object.

You can **only modify** the value of those properties. Do not change the name of the property or delete it. If you change the name, then it is treated as a new **user property**. The old property of Extended PolledData is still retained. Any extra property you add via this dialog box is added as a **user property**. When an Extended PolledData is deleted, its associated user properties are also deleted.



**Warning:**

1. There is no way to differentiate between the **Extended PolledData properties** and **User properties** in the **PolledData Additional properties** dialog.
2. You can only **Modify** the extra fields in an **Extended PolledData**. But, you can **Add / Modify / Delete user properties** of a Statistic.

## Active State of PolledData

If you disable (unchecked) the **active** property, the data collection will not take place for the Statistic. Irrespective of the state of the ManagedObject, PollingObject, and agent, the Statistic will be inactive. This is the default behavior.

If you want to activate or deactivate data collection for the Statistic based on the status of ManagedObject, PollingObject, and agent then a different approach has to be adopted. This is a new feature that can be enabled or disabled as per the need.

This section explains how the status of PolledData (Statistic) is affected by various factors mentioned above and what can be done.

Whether or not the data collection is to take place for a PolledData is determined by the following:

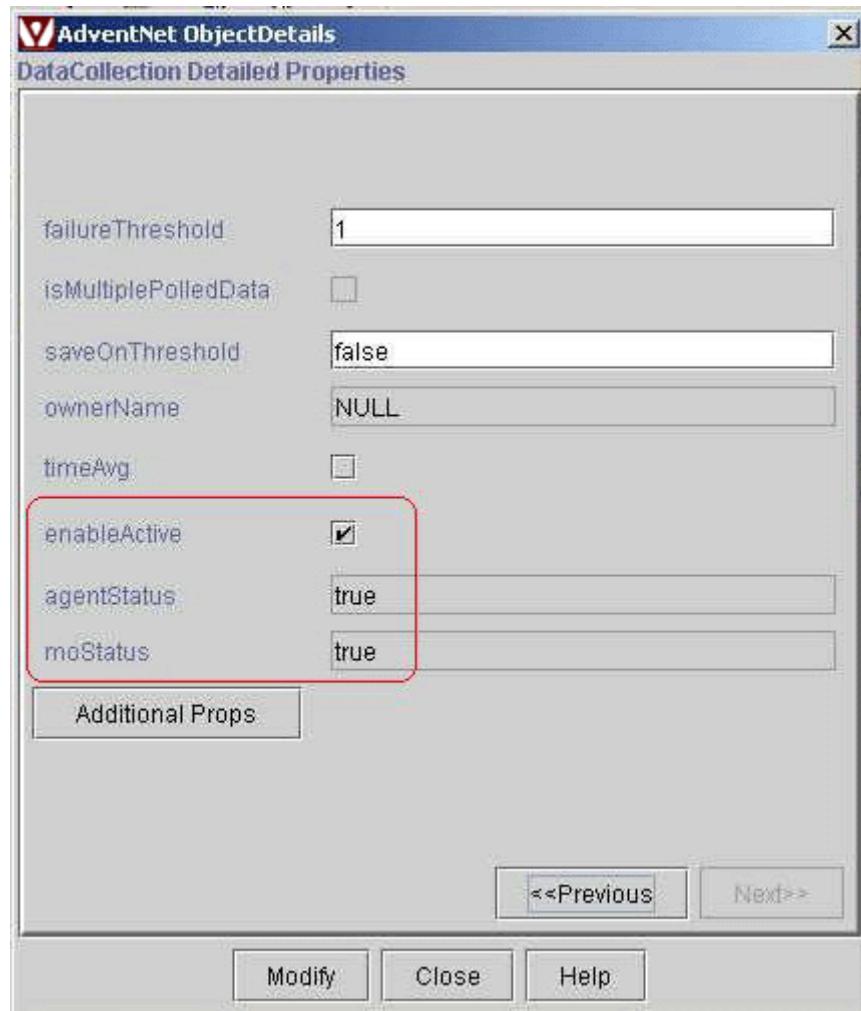
1. PollingObject Status
2. ManagedObject Status
3. Agent Status
4. PolledData status
  - **PollingObject status**, when set **false**, indicates that data collection must not take place for all the PolledData created via that PollingObject.
  - **ManagedObject**, when **unmanaged**, indicates that no data collection should happen for its associated PolledData.
  - When required data collection for an **Agent** is stopped using some system calls.
  - In addition, you have the choice to stop the data collection for a particular PolledData (**User's choice**).

The final **Active** state of the PolledData is an **AND** operation of the above-mentioned four factors. That is, only when all these four factors result in **true**, the PolledData will be active and data collection will be done for it. The following matrix illustrates the same:

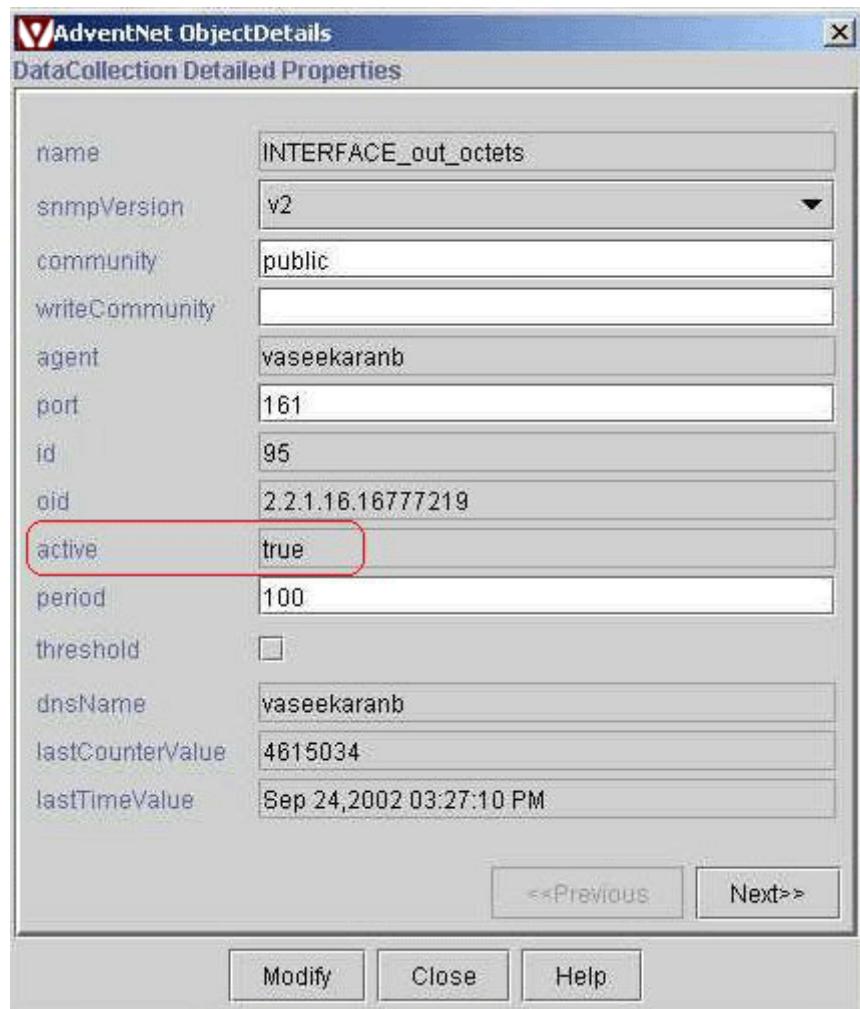
<b>PollingObject Status</b>	<b>ManagedObject Status</b>	<b>Agent Status</b>	<b>User's Choice</b>	<b>Active State of PolledData</b>
True	True	True	True	<b>True</b>
True	True	True	False	<b>False</b>
True	True	False	True	<b>False</b>
True	False	True	True	<b>False</b>
False	True	True	True	<b>False</b>

If this feature is enabled in your setup, you will notice the following changes in the Web NMS Client.

In **Add Statistic** and **Modify Statistic** forms, you can specify your choice for data collection using the check box labeled **enable Active**.



The status of the agent and MO is displayed in a non-editable text box labeled **agentStatus** and **moStatus**. PollingObject status is not displayed there. If all these four are **true**, the non-editable text box labeled **active** is set to **true**.

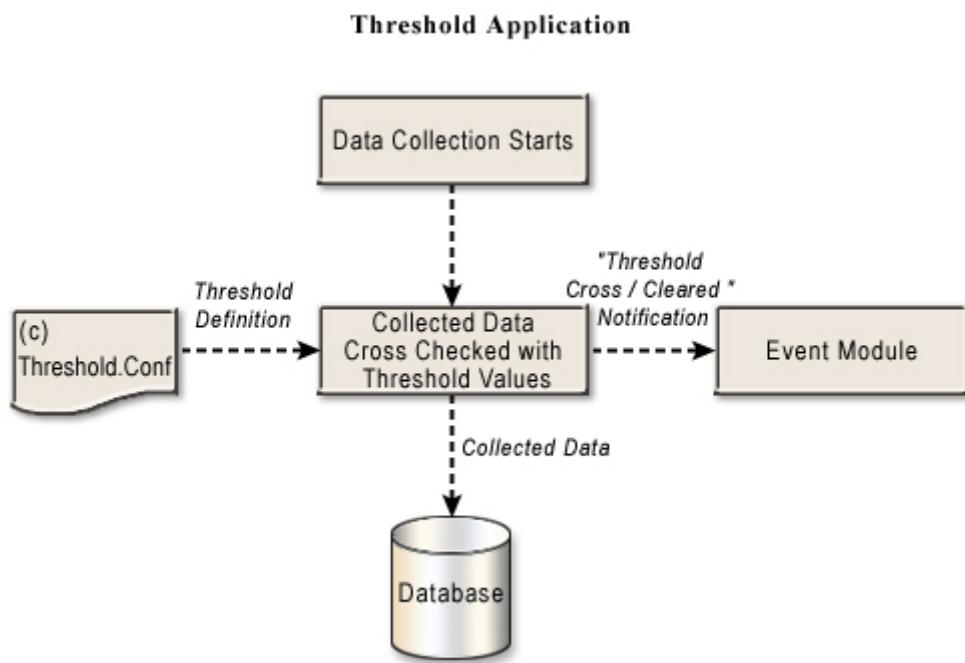


## 6.7.4 Defining Thresholds

- About Thresholds
- Types of Threshold
- Threshold Event Generation
- Defining Multiple Thresholds
- Tips for Creating Threshold

### About Thresholds

Threshold is a value. You associate the Threshold to a Statistic (PolledData). When data is collected for that Statistic, it is compared with the associated Threshold value. If the collected data value does not suit the Threshold value then it indicates that this kind of data might lead to poor performance of the device or network. Here, the term "suit" is used as you can set up a Threshold value along with a level, such as the maximum value, the minimum value, and equal value.



Threshold Level	Description
Max	Assume you create a Threshold with value 100 and level as Maximum. The collected data being greater than this value indicates a problem.
Min	Assume you create a Threshold with value 100 and level as Minimum. The collected data being lesser than this value indicates a problem.
Equal	Assume you create a Threshold with value 100 and level as Equal. The collected data being equal to this value indicates a problem.

These Threshold values act as checkpoints and help in monitoring the collected data.

## Threshold Types

Thresholds in Web NMS Performance modules are of three kinds :

- Thresholds for Long values
- Thresholds for String values
- Thresholds for Percentage values

### Threshold for Long Values

Threshold can be associated with Data identifiers for which the collected data is of type long. Some of such sample Data identifiers are IfAdminStat, IfOperStat, etc in RFC 1213 MIB. The value you provide for this Threshold will be compared as it is with the data collected for the identifier.

### Threshold for String Values

Threshold can be associated with Data identifiers for which the collected data is of type string. One of such sample identifiers is SysDescr. You may wish to monitor a change in system description and hence use String Thresholds.

### Threshold for Percentage Values

Assume that depending upon the Toner level you want to set the number of pages to be loaded in a printer. When the toner level is 80% of the number of pages to be printed, you may like to be notified.

To achieve this, create a Percentage Threshold with a value 80. Collect data for the Statistics "Toner level" and "Number of pages in the printer". Divide "Toner level" by "Number of pages in the printer" and find percentage. If the resultant value exceeds Threshold value (i.e., 80), then you will receive notification.

Actually, you are associating the second Statistic with the Threshold definition itself. Hence,

1. Data is collected for first statistic.
2. When compared with the Threshold value, if the Threshold type is percentage (for the second statistic) data is collected.
3. Both will be divided and the result will be multiplied by 100, thus giving a percentage.
4. This resultant value will be compared with 80, i.e., Threshold value.



**Note:** The Statistics used for percentage calculation must be of same data type. **Example:** If Statistic one is Counter type then Statistic two should also be of type Counter.

## Threshold Event Generation

The notification which you receive when the collected value exceeds Threshold value is in the form of a **Threshold Event**. An event is an occurrence of some action. Hence, whenever Threshold value is exceeded, a Threshold event is generated (handled by Web NMS Fault module).

Also, every Threshold event is associated with a **Severity** to denote the criticality of the situation. **Example:** Critical severity could indicate that immediate attention is needed on data collection, etc.

For information on viewing Thresholds, refer to Monitoring Performance Using Thresholds section in User Guide.

## Defining Multiple Thresholds

You can associate multiple thresholds with a single Statistic. Doing so helps you in having control over every collected value. For example, you can configure such that if the collected value is above 10, the severity is minor. If collected value is above 20, severity is major and so on. In such a case

1. Until a threshold reaches its reset value, it will remain in that severity state. As soon as it reaches the reset value, the threshold is reset and waits for the collected data to exceed its limit again.
2. If another threshold exists of lower severity and if the collected data falls in its limits then that threshold will generate the message.
3. If a threshold exists with higher severity, then the higher severity threshold will take precedence and its message will be displayed. The threshold with lower severity loses its importance and will not be generated until the threshold with higher severity reaches reset state.

## Tips for Creating Threshold

Assume you want to create thresholds for a Router in your network.

1. Identify the Statistic.
2. Once you've decided on the Threshold Statistic, establish baseline values. This can be decided by polling using MIB Browser.
3. After a week, review the data to determine what values are normal for your router.
4. Use the normal values to determine what the highest acceptable values or thresholds would be.
5. A good rule of thumb is to set your thresholds 10-20 percent larger than the maximum values.
6. The threshold values for any Statistic may be applied uniformly across all routers, or they could be customized for groups of routers that have similar characteristics such as core, distribution, and access.
7. You also need to decide on appropriate notification for threshold violations. Because violations are not considered hard errors, immediate notification is unnecessary. Logging all threshold values and reviewing them daily, usually works well. It is important to investigate repeated threshold violations to determine if a problem can be corrected or if threshold values are too low.

## 6.7.4.1 Using User Interface

- Adding Thresholds
- Modifying Thresholds
- Deleting Thresholds

### Adding Thresholds

#### To add Threshold

1. In Web NMS Client, choose **Performance > Configured Collection** from the tree.
2. Select the Statistic from the **Configure Collection** panel.
3. From the **Edit** menu, choose **Threshold > Add Threshold** or press **Ctrl+T**. The **Threshold Properties** dialog box is displayed.
4. Specify a name for the Threshold in the **Name** field.
5. There are 3 tabs, namely **long**, **string**, and **percentage**. For information on the types, refer to the Types of Threshold section.

Specify appropriate values. For information on each of the fields, refer to the following table.

Property	Description
Severity (Trigger Severity)	A string to emphasize the importance of the event generated when Threshold value exceeds. By default, following severity strings have been defined: <b>Critical</b> , <b>Major</b> , <b>Minor</b> , <b>Warning</b> , <b>Clear</b> , <b>Info</b> , and <b>Unknown</b> .
Category	Any happening in a network can be captured and appropriate name can be given to the event generated on such happenings. For example, when Managed Objects are added into database, an event can be generated. This event can be named as <b>AddMOevent</b> . Similarly, generated Threshold events can be named by the developer. This name will be used by Fault module for Event handling and for appropriate notification. By default, the word <b>Threshold</b> is used for identifying Threshold events.
Threshold Type	This indicates the type of Threshold value you are going to specify. Possible values are Max, Min, or Equal. <b>Max:</b> If Collected value exceeds Threshold value, an event is generated. <b>Min:</b> If Collected value is less than Threshold value, an event is generated. <b>Equal:</b> If Collected value is equal to Threshold value, an event is generated.
Threshold Value	Specify an integer value which can be interpreted in two ways: <ol style="list-style-type: none"> <li>1. In case of Threshold defined for Long values, the data collected for the OID is compared with this value.</li> <li>2. In case of Percentage Thresholds, the result of (first OID / second OID) * 100, i.e., a percentage value, is compared with this value.</li> </ol>
Rearm Value	Specify an integer which denotes that when the collected value or calculated value (in case of % thresholds) reaches the Rearm value, the violated Threshold is brought back to normalcy and a clear event is generated.

Property	Description
Reset Severity	When Threshold is reset, you can specify the severity by which it should be denoted.
Allowed Values	Specify a string which is compared with the string collected data. If both matches, Threshold event is generated. Possible values are <ul style="list-style-type: none"> <li>• simply a string, e.g., router5</li> <li>• comma-separated list, e.g., router1and router2</li> <li>• using wild card character e.g. router* where * (asterix) indicates any number of characters and any character.</li> </ul>
Disallowed Values	Specify a string which is compared with the collected string data. If both matches, then Threshold event is generated denoting a <b>reset</b> of Threshold.
Object ID	Specify the Object Identifier for which the data is to be collected in case of Percentage Thresholds. Example: 2.2.1.16.1
Object ID Type	Choose the type of Data identifier - Node, Interface, or Multiple.  <b>Warning:</b> The type of identifier you choose here should be the same as that of the identifier on which this Threshold is going to be applied. Otherwise, when division of the two values take place, invalid resultant value will be generated.
Message	Specify a string that will be displayed in the Event panel of Fault module when Threshold value is exceeded.
Clear Message	Specify a string that will be displayed in the Event panel of Fault module when Threshold is reset (cleared).
Send Clear	Only when this option is selected, Clear events will be generated on Threshold reset. Otherwise the Threshold will be reset and you will not be aware (as no information will be displayed in Event panel of Fault module).

5. Click **Add**.

## Modifying Thresholds

### To modify Threshold

1. In Web NMS Client, choose **Performance > Configured Collection** from the tree.
2. Select the Statistic from the **Configure Collection** panel.
3. From the **Edit** menu, choose **Threshold > Modify Threshold** or press **Ctrl+X**. The **Threshold Properties** dialog box is displayed (only if a Threshold exists for the selected Statistic).
4. Make appropriate changes. For information on each of the fields, refer to the above-given table.
5. Click **Modify**.

## Deleting Thresholds

### To delete Threshold

1. In Web NMS Client, choose **Performance > Configured Collection** from the tree.
2. Select the Statistic from the **Configure Collection** panel.
3. From the **Edit** menu, choose **Threshold > Remove Threshold** or press **Ctrl+R**. A confirmation is asked (only if a Threshold exists for the selected Statistic).
4. Click **Yes** to delete the Threshold.

## 6.7.4.2 Using Configuration File

---

- Severity Constants
  - Threshold for Long Value
  - Threshold for String Value
  - Percentage Threshold
- 

You can create thresholds using the configuration file **Threshold.conf** located in the <Web NMS Home/conf> directory. Define the Threshold properties using the tag **<THRESHOLD> ... </THRESHOLD>** in this file. Ensure to restart the server if you have made configurations in this file.

### Severity Constants

The Severity levels used for Threshold events are predefined and their corresponding integer values are given below. Use these values while specifying the severity in **Threshold.conf**.

Severity Constant	Value
Critical	1
Major	2
Minor	3
Warning	4
Clear	5
Info	6
Unknown	0

### Threshold for Long Value

```
<THRESHOLD
    name="IfInOctect-critical"
    kind="long"
    severity="1"
    category="Threshold"
    thresholdType="Max"
    thresholdValue="20000"
    rearmValue="18000"
    message="Threshold exceeded"
    clrMessage="Threshold reset"
    sendClear="true" />
```

### Threshold for String Value

```
<THRESHOLD
    name="threshold2"
    kind="string"
    allowed="router1,router2"
    disAllowed="router5"
    category="Threshold"
    message="Threshold exceeded"
    triggerSeverity="1"
    resetSeverity="5"
    clrMessage="Threshold reset" />
```

## Percentage Threshold

```
<THRESHOLD  
    name="threshold3"  
    kind="percentage"  
    oid="2.2.1.16.1"  
    oidType="node"  
    severity="1"  
    category="Threshold"  
    thresholdType="Max"  
    thresholdValue="60"  
    rearmValue="55"  
    message="Threshold exceeded"  
    clrMessage="Threshold reset"  
    sendClear="true" />
```

### 6.7.4.3 Associating Threshold with Statistics

- Associating Thresholds with Statistics
- Associating Thresholds with PolledData in PollingObject

#### Associating Thresholds with Statistics

Assume you have created Statistics using the Add Statistic option.

##### To add Thresholds to such a Statistic

1. In Web NMS Client, choose **Performance > Configured Collection** from the tree.
2. Select the Statistic on the right-side **Configured Collection** panel.
3. From the **Edit** menu, choose **Modify Statistic**.
4. Select (tick) the **Threshold** field.
5. Click **Next**.
6. In the thresholdList field, specify the Threshold names.
7. Click **Modify**.

Once you associate the Threshold to the Statistic, monitoring starts for any data collected for that Statistic.



**Note:** After adding a list of Thresholds to the Statistic, if you do not want to monitor the collected data for a while, clear (uncheck) the **Threshold** field. This temporarily stops applying Thresholds on the Statistic.

#### Associating Thresholds with PolledData in PollingObject

##### To associate Thresholds to the PolledData that are created using Polling Object

1. In Web NMS Client, choose **Performance > Configured Collection** from the tree.
2. From the **Edit** menu, choose **Polling Objects > Modify Polling Objects**. The **Poll Details** dialog box is displayed.
3. Skip the first two screens.
4. In the third screen, click **Modify**.
5. Select (tick) the **Threshold** field.
6. From the **Available Thresholds** drop-down box, choose Threshold. These Thresholds are defined in the **Threshold.conf**. Multiple Thresholds can be configured by choosing them one by one.

## 6.7.5 Clearing the Data

Data collected from devices is stored either in STATSDATA table (default table defined by Web NMS) or in user-defined tables. The tables are created on a daily basis (if % was appended to table name when it was defined). Later, if they are not required, they can be removed from the database. Otherwise, it occupies space and may further create problems while storing new tables.

Hence, it is better to perform a periodic clean up of such tables. But ensure that before removing those tables you generate reports on them so that you do not lose the data. You can use this later for analyzing the trend in network performance.

To perform this cleanup operation, Web NMS provides a **Statistics Table Cleanup Policy**. For complete information, refer to Statistics Table Cleanup Policy section under the Viewing Default Policy Details topic.

## 6.7.6 Setting User Privileges

You can prevent a user from accessing certain data in the Web NMS Client and also confine him to viewing and working on only selected performance information. This can be achieved using the **Custom View Scope** mechanism of the Security Management. For more information, refer to Managing Custom View Scopes.

This topic provides an example based on which you can create your own Custom View Scopes for Performance views.

### Example

Assume that there are two users with the following privileges. These users can view only the performance details of hosts that start with 's'.

**User1:** View Thresholds list and View Polling objects

**User2:** View Thresholds list, View Polling objects, and Add Statistics

### Procedure

1. In Web NMS Client, from the **Tools** menu, choose **Security Administration**. The **Security Administration** tool is displayed.
2. Add new user **User1** and **User2**.
3. Add new group **Group A**.
4. Assign required permissions for the Group.
5. Assign the two new users **User1** and **User2** to **Group A**.
6. Set the Scope Criteria.
  - Select the **Group A** on the **Security** tree.
  - Click the **Custom View Scope for Group** tab on the right-side frame.
  - From the **Custom View Scope for Group** drop-down box, choose **Stats Admin**.
  - Click **Add AuthorizedScope**. The **Scope Settings** dialog box is displayed. Enter the **Name** as **Scope A**. From the **Name** drop-down box, select the property as **agent** and enter the **Value** as **s\***.
  - Click **OK**.

After executing this example, log in to the Web NMS Client using the newly added user names. Your Client displays only performance details of devices whose host name starts with **S**.

## 6.7.7 Configurable Parameters

The startup options of the Performance Management module can be modified by editing the parameters of **Collector** process in the **NmsProcessesBE.conf** file located in the <Web NMS Home>/conf directory.



**Note:** If you have configured any of the parameters, ensure to restart the Web NMS Server.

The parameters that can be configured by administrators after deployment are listed below. For information on each of these parameters, refer to Performance Server Startup Options topic in Developer Guide.

- To specify the time after which data collection should start - DATA\_COLLECTION\_STARTUP\_DELAY
- To specify table cleanup periodicity - CLEAN\_DATA\_INTERVAL
- To specify the time after which the Status Poll should start - STATUS\_POLL\_DELAY
- To facilitate viewing of debugging messages in logs - DEBUGGING\_MODE
- To stop data collection - DATA\_COLLECTION
- To stop status polling - STATUS\_POLLING

## 6.8 Security Management

This chapter discusses Security Management. It describes the various elements associated with security, such as groups, users, and operations (permissions).

Security is the assurance of legitimate use, maintenance of confidentiality, data integrity, and the ability to audit the network management operations. It involves identifying the assets, threats, and vulnerabilities of the system, and taking protective measures that, if not done, might lead to unintended use of the system.

The Security Administration module enables you to manage Web NMS Server security information. This security information is stored in the database and in a configuration file, namely **securitydbData.xml** located in the <Web NMS Home>/conf directory.

This chapter helps the Web NMS administrator to create new users or new groups of users, enabling the administrator to control the different security levels of Web NMS. On performing this, the users are allowed to see only the required information in the Web NMS Clients over which they can do the allocated operations.

After logging in to the Web NMS Client, all the operations available to a user are based on the group to which the specific user belongs. Therefore, User Administration is a prime function of the administrators.

A Web NMS administrator can manage the following functions:

- Provide group-based authorization where users can be assigned to groups that have configured levels of authorization, and that provide specific authorizations to a user.
- Provide fine-grained access control for specific groups, views, and operations.
- Limit the access for some users to specific sub-sets of objects or instances (for example, user access can be limited to a specific kind of device).

This chapter explains:

- 
- Managing Groups
  - Managing Users
  - Managing Operations
  - Authorization for Security Operations
  - Configurable Parameters
  - An Example
- 



This chapter explains Security Administration operations that you can perform in an Application, Applet, or Web Start Client. For information on Security Administration in Web Client, refer to the Working with Web Client chapter in User Guide.

## 6.8.1 Managing Groups

A group is a logical collection of users grouped together to access common information or perform similar tasks. Thus, any administration done for the group is reflected in the individual members (or users) of the group.

Web NMS enables you to organize different types of users into groups so they can be classified by a set of common operations. By providing specific permissions to various groups, you can save time when creating new users.

This section provides step-by-step instructions for the following tasks:

---

- Adding Groups
  - Assigning Users to Groups
  - Deleting Users from Groups
  - Configuring Authorized Scopes
  - Managing Custom View Scopes
  - Deleting Groups
-

## 6.8.1.1 Adding Groups

You can add new groups when you want to provide a set of permissions that are different from an existing group.

### To add a group

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.
- The **Security Administration** window is displayed.
2. In **Security Administration** window, perform any of the following procedure.
  - o From **File** menu, choose **New > AddGroup**.
  - o Press **Ctrl+Shift+G**.
  - o Click **AddGroup**.
  - o Right-click the **Groups** node on the **Security** tree (located at the left side of **Security Administration** window) and click **AddGroup**.

The **Groups Wizard** is displayed.

3. Type the group name and click **Next**. The **Operations Tree Root** is displayed. For information on each of the operations, refer to Understanding Default Operations.
4. Click **Finish**.

The new group is added in the **Groups** node in the **Security** tree.

### See Also

---

---

- Assigning Operations for a Group
- 
-

## 6.8.1.2 Assigning Users to Groups

By assigning users to groups, you can limit access to specific sub-sets of the Web NMS Clients. For example, user access can be limited to specific types of devices. To provide group-based permissions, users are assigned to specific groups. These groups provide specific permissions and levels of permissions to the assigned users.

### To assign a user to a group

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.
2. The **Security Administration** window is displayed.
3. From the **Security** tree, click the group to which you need to assign users.
4. Click **Members** tab displayed on the right side.
5. Click **Setting Users**. The **Select Users** window is displayed.
6. To assign a user to a group, click the user in **All Users** and click **>**. For assigning more than one user, do a multiple selection using **Shift** or **Ctrl** buttons.
7. To unassign a user, click the user in **Selected Users** and click **<**.
8. Click **Ok**.

The users assigned to the group is displayed in **Members for** list in **Members** tab.

### 6.8.1.3 Deleting Users from Groups

#### To delete a user from a group

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.
- The **Security Administration** window is displayed.
2. From the **Security** tree, click the group to which you need to assign users.
3. Click **Members** tab displayed on the right side.
4. Click **Setting Users**. The **Select Users** window is displayed.
5. Click the user to be deleted in **Selected Users** and click <.
6. Click **Ok**.

## 6.8.1.4 Configuring Authorized Scopes

Authorized Scopes (or Authorized Views) are independent entities that store the real authorization information. Scopes are associated with the actual operations of a group and with specific properties to which the users have access. Scopes are used to set limits to a permission by applying one or more properties to a group permission.

The set of properties are applicable only when the properties are true. For example, if you assign network=192.168.4.0 to a property, the scope of that associated operation is applicable only to this network.

This section provides step-by-step instructions for the following tasks:

---

- Adding Scopes
  - Changing Scopes
  - Deleting Scopes
- 

### Adding a Scope

You can add a scope to permission when you want to identify a specific object or set of properties to which the group has permissions.

#### To add a scope

1. In the Application Client, perform any of the following procedure.
  - From **Tools** menu, choose **Security Administration**.
  - Press **Alt+S**.The **Security Administration** window is displayed.
2. From the **Security** tree, click the desired group.
3. Click **Permitted Operations for Group** tab on the right side. The operations set for the selected group is displayed.
4. Click the operation for which you need to set a scope and click **Setting Scope**. The **Scope Settings** dialog box is displayed.
5. In the **Name** and **Value** fields, type the property name and value for the scope of the selected operation. For example, name is *network* and its value is *192.168.1.0*.
6. Click **Add**.
7. Click **Ok**.

To add more scopes, repeat steps 3 to 6.

### Changing Scopes

You can change the scope of a permission when you want to change or identify a specific object to which the group has permissions.

#### To change a scope

1. In the Application Client, perform any of the following procedure.
  - From **Tools** menu, choose **Security Administration**.
  - Press **Alt+S**.The **Security Administration** window is displayed.
2. From the **Security** tree, click the desired group.

3. Click **Permitted Operations for Group** tab on the right side. The operations set for the selected group is displayed.
4. Click the operation for which you need to change a scope and click **Setting Scope**. The **Scope Settings** dialog box is displayed.
5. Click the scope to modify.
6. Click **Edit**.
7. In the **Name** and **Value** fields, type the property name and value for the scope of the selected operation.
8. Click **Edit**.
9. Click **Ok**.

## Deleting Scopes

You can delete a scope when you no longer want to specify certain properties for the permission.

### To delete a scope

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.The **Security Administration** window is displayed.
2. From the **Security** tree, click the desired group.
3. Click **Permitted Operations for Group** tab on the right side. The operations set for the selected group is displayed.
4. Click the operation for which you need to delete a scope and click **Setting Scope**. The **Scope Settings** dialog box is displayed.
5. Click the scope to delete.
6. Click **Delete**.
7. Click **Ok**.

## 6.8.1.5 Managing Custom View Scopes

Setting **Custom View Scopes** (CVS) for groups enables you to filter the objects that are to be displayed in the Web NMS Clients and on which a user is permitted to do the respective authorized operations. By specifying the custom view scope criteria, you can ensure that users can view only the data for which they have authorization to perform these operations.

This section provides step-by-step instructions for the following tasks:

- Adding Authorized Custom View Scopes
- Assigning Authorized Custom View Scopes
- Removing Authorized Custom View Scopes from Groups
- Changing Authorized Scope Properties
- Deleting Authorized Custom View Scopes
- See Also

---

### Adding Authorized Custom View Scopes

You can add an authorized Custom View Scope to a group to ensure the members of a group can view only the authorized data.

#### To add a custom view scope

1. In the Application Client, perform any of the following procedure.
    - From **Tools** menu, choose **Security Administration**.
    - Press **Alt+S**.
- The **Security Administration** window is displayed.
2. From the **Security** tree, click the desired group.
  3. Click **Custom View Scope for Group** tab on the right side.
  4. From **Custom View Scope Name** drop down box, choose the module.
  5. Click **Add AuthorizedScope**. The **Scope Settings** dialog box is displayed.
  6. Enter the **Authorized Scope Name** in the **Name** field.
  7. From the **Name** drop-down box, select the **Property** name. This drop-down box lists the property names (which can be used for creating the authorized scopes) specific to each of the Custom View Scope. For instance, selecting the **Events** Custom View Scope and clicking **Scope Settings**, provides you with the property names of *Event Objects*.
  8. Enter the value for the property in **Value** field. To identify more than one property value, separate each value according to the appropriate operator in the following Value Operators table:

Value Operator	Description
* (Asterisks)	Use asterisk to filter on a match of zero or more characters.  <b>Example:</b> To view all objects starting with the name <b>test</b> , set the property key as <b>name</b> and the value as <b>test*</b> .
! (Exclamation Mark)	Use exclamation mark to filter the search using the <b>NOT</b> operator.  <b>Example:</b> To view all objects whose names do not start with <b>test</b> , set the property key as <b>name</b> and value as <b>!test*</b> .

Value Operator	Description
,	Use comma to filter objects where a single property key has different values.  <b>Example:</b> To view all objects with names starting with <b>abc</b> or <b>xyz</b> , set the property key as <b>name</b> and value as <b>abc*,xyz*</b> .
&&	Use ampersand to filter objects where a single value should be matched with many patterns.  <b>Example:</b> To view all objects with names starting with <b>abc</b> and ending with <b>xyz</b> , set the property key as <b>name</b> and value as <b>abc*&amp;&amp;*xyz</b> .
\	Use back slash to filter objects when the name of the object itself contains a comma. This character is called an escape sequence because it avoids searching for objects, as if they had two different names.  <b>Example:</b> To view an object with name <b>a,b</b> , set the property key as <b>name</b> and the value as <b>a\,b</b> .
<between> value1 and value2	Use greater than and less than signs to filter objects with numeric values within a specific range.  <b>Example:</b> If object names with a poll interval value ranging between or including 300 and 305 are required, set the property key as <b>pollinterval</b> and value as <b>&lt;300 and 305&gt;</b> .  Note that the first number is smaller than the second number. Only the values in between the given values, including the limits, are matched.

9. Click **Add**. This adds the Authorized Scope for the selected Custom View Scope of the group. You can add more than one property criteria based on your requirement.
10. On adding the properties, click **Ok** for making a permanent store.

## Assigning Authorized Custom View Scopes

After you have created an authorized Custom View Scope for a group, you can assign it to other groups as necessary.

### To assign an authorized custom view scope

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.
 The **Security Administration** window is displayed.
2. From the **Security** tree, click the desired group.
3. Click **Custom View Scope for Group** tab on the right side.
4. Click **Assign AuthorizedScope**. The Select **AuthorizedScopes** window is displayed.
5. Click the desired Authorized Scope from **All AuthorizedScopes** and click **>**.
6. Click **Ok**. The selected scopes are displayed in both the **All AuthorizedScopes** list and in the **Selected AuthorizedScopes** list.

## Removing Authorized Custom View Scopes from Groups

You can remove an authorized Custom View Scope from a group when it is no longer valid for that group. By removing the Custom View Scope, the properties themselves are not changed nor is the Custom View Scope deleted from the database.

### To remove an authorized custom view scope

1. In the Application Client, perform any of the following procedure.
    - o From **Tools** menu, choose **Security Administration**.
    - o Press **Alt+S**.
- The **Security Administration** window is displayed.
2. From the **Security** tree, click the desired group.
  3. Click **Custom View Scope for Group** tab on the right side.
  4. Click **Assign AuthorizedScope**. The **Select AuthorizedScopes** window is displayed.
  5. Click the desired Authorized Scope from **Selected AuthorizedScopes** and click <.
  6. Click **Ok**.

## Changing Authorized Scope Properties

After you have added properties to an authorized Custom View Scope, you can make changes as appropriate.



If you have assigned the authorized Custom View Scope to other groups, any changes to the Custom View Scope will affect those groups as well.

### To change an authorized scope properties

1. In the Application Client, perform any of the following procedure.
    - o From **Tools** menu, choose **Security Administration**.
    - o Press **Alt+S**.
- The **Security Administration** window is displayed.
2. From the **Security** tree, click the desired group.
  3. Click **Custom View Scope for Group** tab on the right side.
  4. Click the Authorized Scope to be modified from **AuthorizedScopes for CV** list.
  5. Click **Set Scope Properties**. The **Scope Settings** dialog box is displayed. For information on adding, modifying, or removing the scope, refer to Configuring Authorized Scope.
  6. Click **Ok**.

## Deleting Authorized Custom View Scopes

When an authorized custom view scope is no longer valid, you can delete it from the database. After this action, you must recreate it if you ever need it again.

### To delete an authorized custom view scope

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.

The **Security Administration** window is displayed.

2. From the **Security** tree, click the desired group.
3. Click **Custom View Scope for Group** tab on the right side.
4. Right-click the Authorized Scope to be deleted from **AuthorizedScopes for CV** list and click **Delete AuthorizedView**.

After confirming that you want to delete the Custom View Scope, it is deleted from the database and from any group to which it was associated.

## See Also

---

Refer to the following topics for information on Authorized Scopes in each of the modules.

- Topology
  - Maps
  - Fault Management
  - Performance Management
  - Provisioning Framework
-

## 6.8.1.6 Deleting Groups

### To delete a group

1. In the Application Client, perform any of the following procedure.
    - o From **Tools** menu, choose **Security Administration**.
    - o Press **Alt+S**.
- The **Security Administration** window is displayed.
2. From the **Security** tree, click the group to be deleted.
  3. Perform any of the following procedures.
    - o From **Edit** menu, choose **Delete**.
    - o Press **Alt+D**.
    - o Right-click the group on the tree and click **Delete**.

To confirm the deletion, click **Yes**. The group is removed from the database.

## 6.8.2 Managing Users

A user is an individual entity which logs on to the Web NMS and is configured to perform only a set of Web NMS-related functions. Before anyone has access to the Web NMS Client, he or she must be added as a user to the Web NMS Server database. After you have created users, you can add them to groups, and/or give them specific permissions unrelated to the group.

This section provides step-by-step instructions for the following tasks:

---

- Adding Users
  - Changing User Profile
  - Assigning Groups to Users
  - Changing User Password
  - Managing Audit Trails
  - Deleting Users
-

## 6.8.2.1 Adding Users

You can add a user whenever you need to provide access to the Web NMS Client. By default, the new user has login permission only. You provide access to various modules by making the user a member of pre-configured groups or by directly assigning permissions to the user.

You can add a new user

---

1. From Application Client
  2. From Web Client
  3. Using Command Line
- 

### Adding User from Application Client

The procedure to add a new user for Application, Applet, or Web Start Client is the same. For more information on Web NMS Clients, refer to Understanding Web NMS Clients in User Guide.

#### To add a new user

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.
2. In **Security Administration** window, perform any of the following procedure.
  - o From **File** menu, choose **New > AddUser**.
  - o Press **Ctrl+Shift+U**.
  - o Click **AddUser**.
  - o Right-click the **Users** node on the **Security** tree (located at the left side of **Security Administration** window) and click **AddUser**.

The **User Administration** wizard is displayed.

3. Type the user name and password in appropriate fields and click **Next**. If no password is specified, the user name is set as the password.
4. In the **User account expiry** section, complete one of the following steps:

By default, the user account never expires.

- If you are providing access for a limited number of days, type the number of days in which the account expires in the **Day(s)** field.
- If the account has no expiration, check the **Account never expires** checkbox.

In the **Password expiry** section, complete one of the following steps:

By default, the user account never expires.

- If the password has an expiration time period, type the number of days in which the password expires in the **Day(s)** field.
- If the password has no expiration, check the **Password never expires** checkbox.

**Note:** Here user account expires and password expires are two different entities. You can give user name and password expiry separately. Password expiry is checked only

when the user tries to login. Whereas the user account expiry check is done at a regular time interval. This time interval check works only if **time\_interval\_for\_security\_scheduler\_in\_ms** parameter in **NmsProcessesBE.conf** file located in <Web NMS Home>/conf directory is configured (in milliseconds). By default, the value is set as '0' whereby scheduler will not be started and the user expiration check will not be done.

Click **Next**.

5. Perform any of the following.

If you are associating the user with an existing group, complete the following steps:

- Check the **Group based permissions** checkbox.
- In **Assign groups for the user**, check the checkboxes next to the groups to which you want to assign the user.

**Tip:** Click the arrow  in the dialog box to display a pop-up window displaying the corresponding permissions for the group. Based on the permissions you can assign groups to the user.

If you want to create a new group to which you want to associate the user, complete the following steps:

- In the **Enter the new group name** field, type a name for the new group.
- Click **Add Group**.

The Assign Permissions dialog box is displayed. For more information about selecting permissions in this dialog box for the new group, see step 4 in the “Changing Group Permissions.”

To directly assign permissions to the user, complete the following steps:

- Check the **Direct assignment** checkbox.
- Click the **Permissions** button.

The **Assign Permissions** dialog box is displayed. For more information on selecting permissions in this dialog box, refer to Assigning Operations.

**Note:** The operations assigned to the user are specific to that particular user alone.

6. When you have finished assigning permissions to the user, click the **Finish** button.

The new user is displayed in the **Security** tree on the left side of **Security Administration** window.

## Adding User Using Command Line

Execute **UserConfig.sh/bat** file located in <Web NMS Home>/bin/admintools directory, from the command line as given below:

```
UserConfig.sh/bat Add <Web NMS Home> UserName Password Group RMI
port number
```

Where,

*UserName* is the user name of the new user.

*Password* is the password to authenticate the user during his login.

*Group* is the group to which the user should belong.

*RMI port number* (optional): The RMI port number of Web NMS. If not specified, the default RMI port number 1099 is set.

### Example

```
UserConfig.sh/bat Add > c:/program files/adventnet/webnms  
guest xyz Admin 1100
```

A new user **guest** is added to **Admin** group with password **xyz** to the database.

### See Also

---

---

- Assigning Operations for a User
- 
-

## 6.8.2.2 Changing User Profile

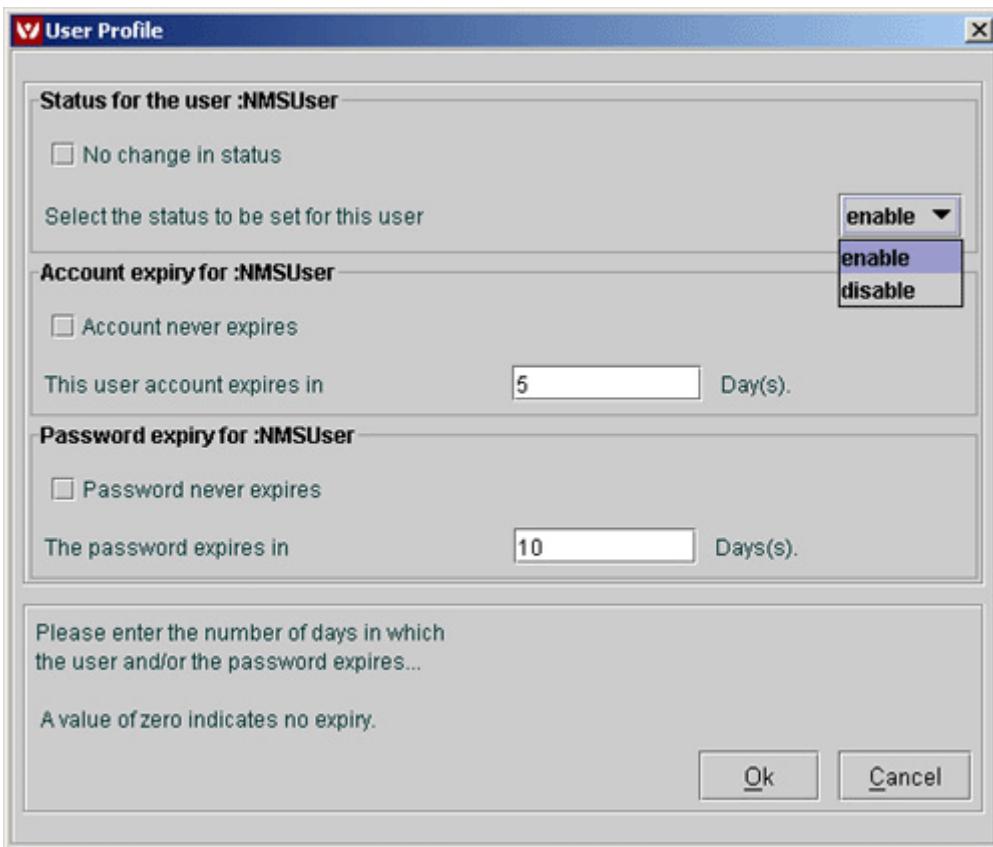
You can change a user's profile when necessary. You might want to change a profile to change the expiration of an account or password.

### To change a user profile

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.

The **Security Administration** window is displayed.

2. In **Security Administration** window, click the user whose profile you need to change on the **Security** tree. The **Security Administration** tabs are displayed on the right-side.
3. Click **User Profile** tab.
4. Click **Setting Profile**. The **User Profile** dialog box is displayed.



5. To enable or disable the user, uncheck **No change in status** check box and from the drop-down box, choose **enable** or **disable** as appropriate.
6. Make changes to account and user expiry as appropriate. For information on the fields, refer to Adding a new user procedure.
7. Click **Ok**.

The Security Administration window displays a Security tree **Groups** and **Users** nodes on the left side. The various types of icons displayed under the **Users** node provide immediate information about the status of a specific user. The following table lists all the icons and explains what it represents.

Icon	Description
	User account is enabled.
	User is disabled and cannot log in until he/she is re-enabled.
	User account has expired.
	User password has expired.
	User has been forced out and cannot log in to the server. This is similar to the disabled user status.
	User login is denied due to continuous unsuccessful login attempts.

## See Also

---

- Deleting Users from Groups
  - Assigning Operations for a User
-

### 6.8.2.3 Assigning Groups to Users

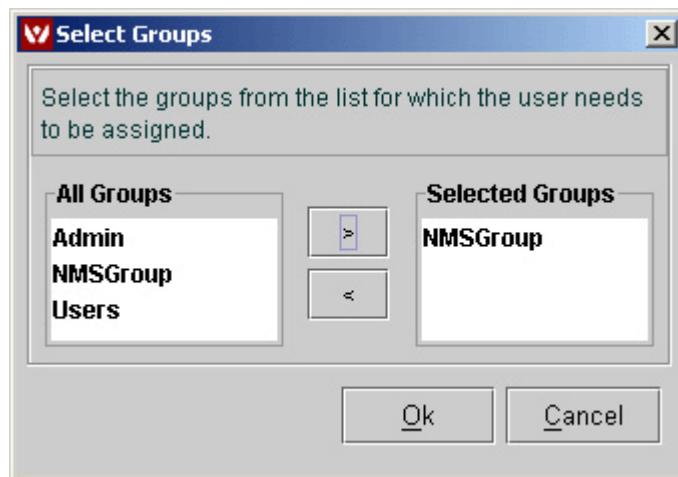
You can assign the users that you have created to already existing groups.

#### To assign groups to users

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.

The **Security Administration** window is displayed.

2. In **Security Administration** window, click the user whose profile you need to change on the **Security** tree. The **Security Administration** tabs are displayed on the right-side.
3. Click **Member Of** tab.
4. Click **Setting Groups**. The **Select Groups** window is displayed.



5. To assign a group to the user, click a group in **All Groups** list and click **>**. For assigning more than one group, do a multiple selection using **Shift** or **Ctrl** buttons.
6. To unassign a group, click the group in **Selected Groups** list and click **<**.
7. Click **Ok**.

The groups assigned to the user is displayed in **Groups for** list in **Members Of** tab.

## 6.8.2.4 Changing User Password

### To change a user password

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.
- The **Security Administration** window is displayed.
2. In **Security Administration** window, click the user whose password you need to change on the **Security** tree. The **Security Administration** tabs are displayed on the right-side.
3. Perform any of the following procedure.
  - o From **Edit** menu, choose **Change Password**.
  - o Press **Ctrl+Shift+C**.
  - o Right-click the user node on the **Security** tree and click **Change Password**.

The **Change Password** dialog box is displayed.

4. Enter the new password in the fields and click **Ok**.

The new password is saved to the Web NMS Server.

## 6.8.2.5 Managing Audit Trails

Audit trails enable you to view the operations that have been performed by a user. The audit trail identifies all operations that have been performed, the time, whether it was successful, category, and audited object. You should periodically clear the trails after they have been reviewed.

### You can:

- View the audit trail details of all the users or a single user.
- Sort the details by user, operation, time, status, category, and audited object by clicking the appropriate column heading.
- Search for audit details based on the properties.
- Clear the audit trails when you no longer need to manage them.

This topic explains:

---

- Viewing Audit Trails of All Users
  - Viewing Audit Trails in Web Client
  - Viewing Audit Trails of a Single User
  - Sorting Audit Trails
  - Searching the Audit Trails
- 

### Viewing Audit Trails of All Users

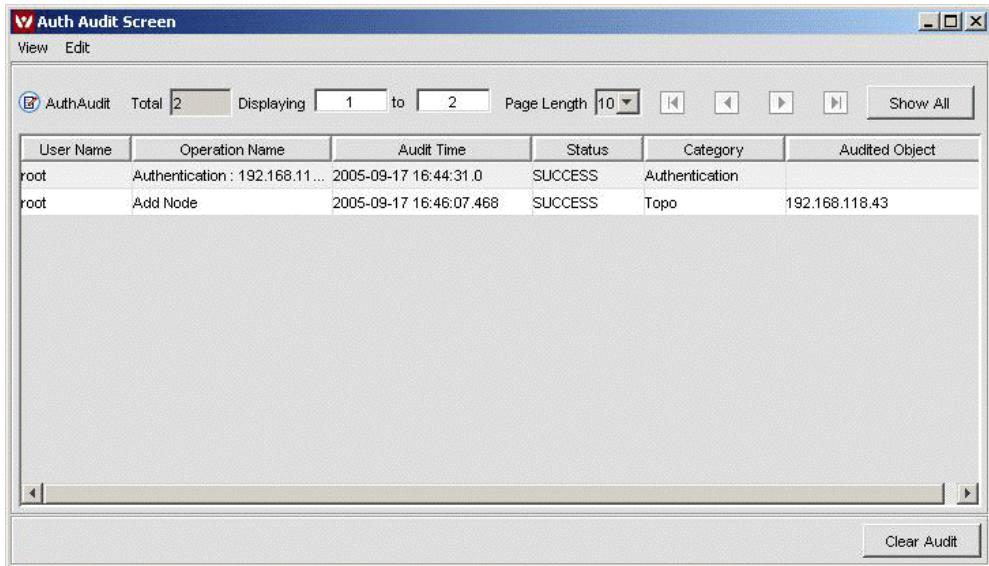
#### To view audit trails of all users

1. In the Application Client, perform any of the following procedure.
  - From **Tools** menu, choose **Security Administration**.
  - Press **Alt+S**.

#### The Security Administration window is displayed.

2. In **Security Administration** window, perform any of the following procedure.
  - From **View** menu, choose **AuditTrails**.
  - Press **Ctrl+Shift+A**.
  - Click **AuditTrails**.

The **Auth Audit Screen** is displayed. Various operations performed by the users along with the status of whether the operation was a success or failure are displayed. The operation category such as Fault, Topo, Provisioning, Configuration, or DEFAULT is also displayed. In the case of operation that involves any objects, such as "Add Node" operation where the object is added, then the object detail is displayed.



3. To sort the list, click the appropriate column heading.
4. To clear an audit trail, click the audit and click **Clear**.

**Tip:** To select a single audit trail, click it, for contiguous audit trails, press and hold Shift key while clicking the appropriate trails, and to select non-contiguous audit trails, press and hold the Ctrl key while clicking the appropriate audit trails.

## Viewing Audit Trails in Web Client

1. Select the **Admin** Tab.
2. Click the **Audit Trails** icon in the **System Administration** panel.

Auth Audit						
Search		Page Length 25 1 to 8 of 8				
		Clear Audit				
#	UserName	Operation	AuditTime	Status	Category	AuditedObject
<input type="checkbox"/>	root	System Administration	2005-09-21 17:46:03.499	SUCCESS	DEFAULT	
<input type="checkbox"/>	root	Authentication : 192.168.117.98	2005-09-21 17:45:53.906	SUCCESS	Authentication	
<input type="checkbox"/>	root	Clear Audit Trails	2005-09-21 17:37:34.365	SUCCESS	DEFAULT	
<input type="checkbox"/>	root	Authentication : 192.168.117.98	2005-09-09 19:31:12.418	SUCCESS	Authentication	
<input type="checkbox"/>	guest	Authentication : 192.168.117.98	2005-09-09 19:23:21.075	SUCCESS	Authentication	
<input type="checkbox"/>	root	Authentication : 192.168.117.98	2005-09-09 19:19:59.776	SUCCESS	Authentication	
<input type="checkbox"/>	root	Authentication : 192.168.111.153	2005-09-09 18:41:03.338	SUCCESS	Authentication	
<input type="checkbox"/>	root	Add Node	2005-09-09 18:39:49.062	SUCCESS	Topo	192.168.118.43

There is provision to search the audit trail details and sort on the desired columns in the Audit Audit page, along with provision for easy page navigation.

## Viewing Audit Trails of a Single User

### To view audit trails of a single user

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.

The **Security Administration** window is displayed.

2. In the Security tree, click the desired user under **Users** node.
3. Click **Audit Trails** in the right click menu.
4. To clear an audit trail, click the audit and click **Clear Trails**.

## Sorting Audit Trails

**To perform client side sorting where the audit trails details in that particular page will be sorted.**

1. Invoke the **Auth Audit** screen.
2. Click on the column header of the property on which the Audit trails have to be sorted holding down the **Ctrl** button.

**To perform server side sorting where the audit trails details in the database will be sorted and displayed in the UI.**

1. Invoke the **Auth Audit** screen.
2. Click on the column header of the property on which the Audit trails have to be sorted.

## Searching the Audit Trails

1. Invoke the **Auth Audit** screen.
2. Press **Ctrl+S**
3. Select the property on which the search has to be performed from the combobox.
4. Select the condition from the combobox.
5. Specify the value in the text box.
6. Click the **Search** button to search the Audit Trails screen.

	<p><b>Note:</b> After viewing the audit details based on the Search results, you can view all the details again in the same page by clicking on the '<b>Show All</b>' button in the top right corner of the <b>Auth Audit screen</b>.</p>
--	---

## 6.8.2.6 Deleting Users

You can delete a user when you no longer want to provide access to the Web NMS Clients.

### To delete a user

1. In the Application Client, perform any of the following procedure.
  - o From **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.
2. In the **Security** tree, click the desired user under **Users** node and perform any of the following procedure.
  - o From **Edit** menu, choose **Delete**.
  - o Press **Alt+D**.
  - o Right-click user node on the tree and click **Delete**.

A confirmation to delete the user is asked. Click **Yes** to delete the user.

## 6.8.3 Managing Operations

The **Operations Tree** contains a list of operations (also referred to as **permissions**) that is provided by default in Web NMS. The operations are logically arranged in a tree structure with parent and child operations. You can add new operations when they are needed and delete obsolete operations.

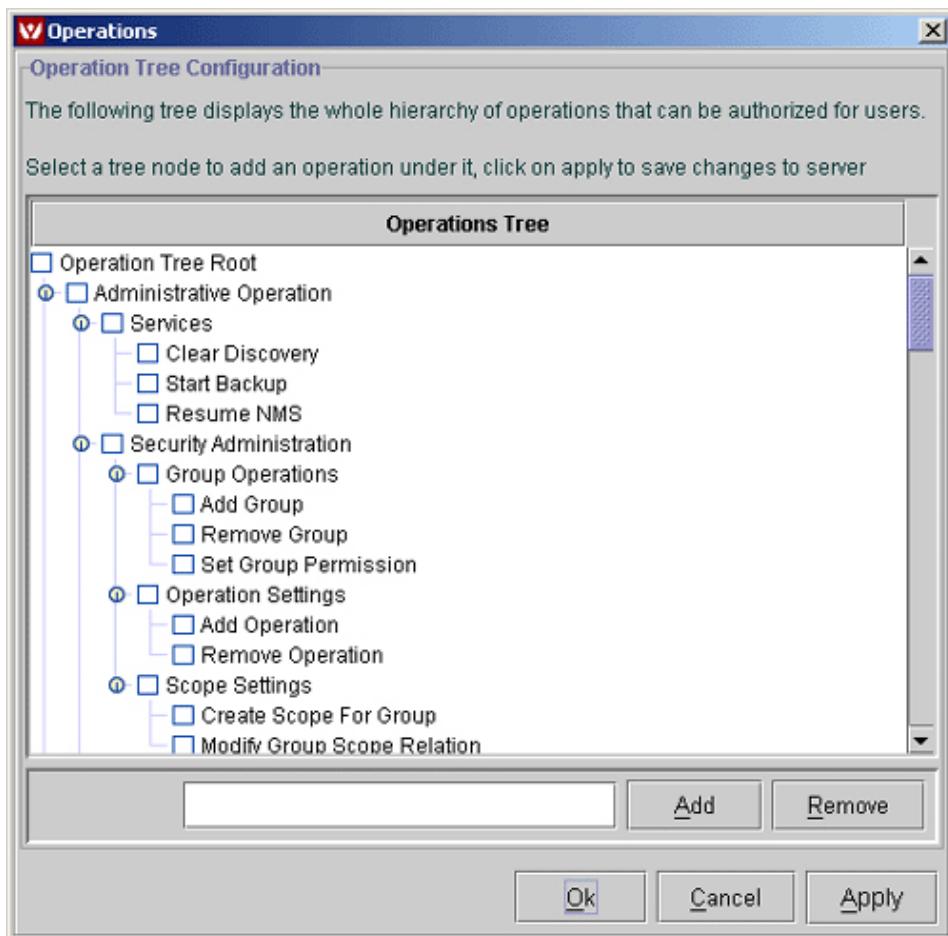
---

- Understanding Default Operations
  - Assigning Operations
  - Adding Operations
  - Deleting Operations
-

### 6.8.3.1 Understanding Default Operations

The **Operations Tree** contains a list of operations that is provided by default in Web NMS. Assigning different operations to different users is an administrative function.

- Administrative Operation
- Events
- Topology
- Policy
- User Administration
- Trap Parsers And Filters
- Alerts
- Configuration
- Maps
- Polling Units
- Polling Object
- Threshold Object
- Poll Filters
- Provisioning



## Administrative Operation

### Services

Operation	Description
Clear Discovery	The discovery process may be stopped due to some unforeseen problems. The Clear Discovery operation is used to resume the discovery process.  Disabling this option prevents the user from resuming the discovery process from the Web Client.
Start Backup	This operation is to start the Web NMS backup process. This operation suspends all the Web NMS Schedulers.  Disabling this operation prevents the user from starting the backup process.
Resume NMS	This operation is performed to resume all Web NMS Schedulers if the backup process has some errors.

### Shutdown Web NMS Server

Disabling this operation prevents the user from shutting down the Web NMS Server. This is applicable to both the Application Client and the Web Client.

### Configure Log Levels

Disabling this operation prevents the user from configuring the log levels (applicable only to Web Client).

### Runtime Administration

Disabling this operation prevents the user from working on the Runtime Administration Tool. For more information on Runtime Administration Tool, refer to Runtime Administration.

### Security Administration

The Security Administration node provides the following security-related operations that can be configured. You can provide permission for users only for certain security operations and restrict the others. For instance, you can provide permission for a user to create a new group but he might not have the option to delete the same. Refer Authorization for Security Operations for more information and an example on how authorization support is provided in the Security Administration UI.

Operation	Description	
Group Operations	Add Group	Disabling this operation prevents the user from adding a new group.
	Remove Group	Disabling this operation prevents the user from removing a group.
	Set Group Permission	Disabling this operation prevents the user from setting permissions or operations to groups.
Operations Settings	Add Operation	Disabling this operation prevents the user from creating new operations in the Operations UI.
	Remove Operation	Disabling this operation prevents the user from removing existing operations from the Operations tree.

<b>Operation</b>		<b>Description</b>
Scope Settings	Create Scope For Group	Disabling this operation prevents the user from adding a new scope or setting the properties of a scope.
	Modify Group Scope Relation	Disabling this operation prevents the user from assigning a scope to a group in the Custom View Scope for Group UI.

## System Administration

Disabling this operation prevents the user from accessing the System Administration page in Application Client and Web Client.

---

## Events

<b>Operation</b>		<b>Description</b>
Event Filters and Parsers	Get Event Parsers	Disabling this operation prevents the user from viewing the existing event parsers in Web NMS Server.
	Set Event Parsers	Disabling this operation prevents the user from modifying or adding a new event parser.
	Get Event Filters	Disabling this operation prevents the user from viewing the existing event filters in Web NMS Server.
	Set Event Filters	Disabling this operation prevents the user from modifying or adding a new event filter.
Event User Operations	Save Events To File	Disabling this operation prevents the user from saving the events in file.
	Print Event View	Disabling this operation prevents the user from printing the list of events.

## Topology

<b>Operation</b>		<b>Description</b>
Modify Object	Start And Stop Discovery	Disabling this operation prevents the user from starting or stopping the discovery process of Web NMS Server.
	Manage And Unmanage Objects	Disabling this operation prevents the user from managing or unmanaging an object or a network element.
Add Network		Disabling this operation prevents the user from adding a new network manually.
Add Node		Disabling this operation prevents the user from adding a new node in the network manually.
Delete Object		Disabling this operation prevents the user from deleting an object or a network element.
Refresh Node		Disabling this operation prevents the user from refreshing a node.

## Policy

Operation	Description
Add Policy	Disabling this operation prevents the user from adding a new policy.
Delete Policy	Disabling this operation prevents the user from deleting an existing policy.

---

## User Administration

Operation	Description
User Configuration	Disabling this operation prevents the user from accessing User Configuration link in Web Client.
Add Users	Disabling this operation prevents the user from adding new users. This is applicable to both the Application Client and the Web Client.
Assign User To Group	Disabling this operation prevents the user from assigning a user to a group. This is applicable to both the Application Client and the Web Client.
Remove Users	Disabling this operation prevents the user from removing a user. This is applicable to both the Application Client and the Web Client.
Remove User From Group	Disabling this operation prevents the user from removing a user from a group. This is applicable to both the Application Client and the Web Client.
Change Password	Disabling this operation prevents the user from changing the password of a user. This is applicable to both the Application Client and the Web Client.
Get List Of Users	Disabling this operation prevents the user from viewing the list of users added. This is applicable only to Web Client (the link to access the list if disabled).
Set User Permission	Disabling this operation prevents the user from setting operations or permissions for existing users. This is applicable to both the Application Client and the Web Client.
Set User Profile	Disabling this operation prevents the user from setting profiles for existing users. This is applicable to both the Application Client and the Web Client.
Clear Audit Trails	Disabling this operation prevents the user from clearing audit trails in Application Client.

---

## Trap Parsers and Filters

Operation	Description
Get Trap Filters	Disabling this operation prevents the user from viewing the existing trap filters using Runtime Administration Tool.
Set Trap Filters	Disabling this operation prevents the user from setting new trap filters using Runtime Administration Tool.
Reload Trap Filters	Disabling this operation prevents the user from reloading the trap filters using Runtime Administration Tool.
Get Trap Parsers	Disabling this operation prevents the user from viewing the existing trap parsers.
Set Trap Parsers	Disabling this operation prevents the user from setting new trap parsers.

## Alerts

<b>Operation</b>		<b>Description</b>
Alert Filters	Get Alert Filters	Disabling this operation prevents the user from viewing existing alert filters.
	Set Alert Filters	Disabling this operation prevents the user from setting new alert filters.
Alert User Operations	Set Alert Annotation	Disabling this operation prevents the user from annotating an alarm.
	Get Alert Details	Disabling this operation prevents the user from viewing the details of an alarm.
	Save Alerts To File	Disabling this operation prevents the user from saving the list of alarms in a file.
	Print Alert View	Disabling this operation prevents the user from printing the alarms.
	Clear Alerts	Disabling this operation prevents the user from clearing the alarms.
	Get Alert Annotation	Disabling this operation prevents the user from viewing the annotation of an alarm.
	Get Alert History	Disabling this operation prevents the user from viewing the history of an alarm.
	Alert Pickup	Disabling this operation prevents the user from picking up an alarm.
	Delete Alerts	Disabling this operation prevents the user from deleting an alarm.

---

## Configuration

<b>Operation</b>	<b>Description</b>
Create Task	Disabling this operation prevents the user from creating new tasks.
Execute Task	Disabling this operation prevents the user from executing tasks.

---

## Maps

<b>Operation</b>	<b>Description</b>
Map Editing Operations	Disabling this operation prevents the user from adding or deleting symbols, links, and containers, grouping symbols, clearing or deleting alarms, and configuring nodes in a map.

---

## Polling Units

<b>Operation</b>	<b>Description</b>
Add Polling Units	Disabling this operation prevents the user from adding polling units or statistics.
Remove Polling Units	Disabling this operation prevents the user from removing an existing polling unit or statistic.
Modify Polling Units	Disabling this operation prevents the user from modifying an existing polling unit or statistic.
Get Polling Unit	Disabling this operation prevents the user from viewing the details of the polling unit or statistic.

## Polling Object

Operation	Description
Add Polling Object	Disabling this operation prevents the user from adding new polling objects.
Modify Polling Object	Disabling this operation prevents the user from modifying existing polling objects.
Delete Polling Object	Disabling this operation prevents the user from deleting polling objects.
Changing Polling Object Status	Disabling this operation prevents the user from changing the status of a polling object.
Get Polling Objects	Disabling this operation prevents the user from viewing the existing polling objects.

## Threshold Object

Operation	Description
Add Threshold Object	Disabling this operation prevents the user from adding new threshold objects.
Modify Threshold Object	Disabling this operation prevents the user from modifying existing threshold objects.
Delete Threshold Object	Disabling this operation prevents the user from removing threshold objects.
Get Threshold Object	Disabling this operation prevents the user from viewing the available threshold objects.

## Poll Filters

Operation	Description
Get Poll Filters	Disabling this operation prevents the user from viewing the existing poll filters in Runtime Administration Tool.
Update Poll Filters	Disabling this operation prevents the user from updating existing poll filters using Runtime Administration Tool.
Reload Poll Filters	Disabling this operation prevents the user from reloading the poll filters using Runtime Administration UI.

## Provisioning

Operation	Description
View TemplateResult	Disabling this operation prevents the user from viewing the results of a provisioning operation in ActivityList view.

### 6.8.3.2 Assigning Operations

You can assign operations (include or exclude privileges) for a group or for a particular user. Assigning operations for a group automatically sets the same privileges for the users in that group.

- Assigning Operations for a Group
- Assigning Operations for a User

---

#### Assigning Operations for a Group

##### To assign operations for a group

1. In the Application Client, perform any of the following procedures:
    - From the **Tools** menu, choose **Security Administration**.
    - Press **Alt+S**.
- The **Security Administration** window is displayed.
2. From the **Security** tree, click the group to which you need to assign operations.
  3. Click the **Permitted Operations for Group** tab displayed on the right side. All operations included or excluded for that group are displayed in the **Operations For Group** list.
  4. Click **Set Permissions**. The **Assign Permissions** window is displayed.
  5. To grant the appropriate permissions, perform any of the following procedures:
    - To include the permissions you want to grant to the group, check the appropriate check boxes (a tick is displayed).
    - To prevent specific permissions from being granted to the group, click the check box until an **x** is displayed in the check box.

Leaving the check box empty for an operation will not be accounted as an authorized operation and it inherits its immediate parent operation permission. For information on each of the operations, refer to Understanding Default Operations.

6. To cancel the changes before closing the window, click **Reset**.
7. Click **Done**.

#### Assigning Operations for a User

##### To assign operations for a user

1. In the Application Client, perform any of the following procedures:
    - From the **Tools** menu, choose **Security Administration**.
    - Press **Alt+S**.
- The **Security Administration** window is displayed.
2. From the **Security** tree, click the user for whom you need to assign operations.
  3. Click the **Permitted Operations for User** tab displayed on the right side. All operations included or excluded for that group are displayed in the **Permissions For User** list.
  4. Click **Set Permissions**. The **Assign Permissions** window is displayed.
  5. To grant the appropriate permissions, complete the following steps:
    - To include the permissions you want to grant to the group, check the appropriate check boxes (a tick is displayed).

- To prevent specific permissions from being granted to the group, click the check box until an **x** is displayed in the check box.

Leaving the check box empty for an operation will not be accounted as an authorized operation and it inherits its immediate parent operation permission. For information on each of the operations, refer to Understanding Default Operations.

6. To cancel the changes before closing the window, click **Reset**.
7. Click **Done**.

### 6.8.3.3 Adding Operations

You can add new operations to the Web NMS Clients. For example, as new sub-applications are added, you might find that the current operations are not adequate for your needs; you can add operations that apply to the new sub-application.

#### To add an operation

1. In the Application Client, perform any of the following procedures:
  - o From the **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.

The **Security Administration** window is displayed.

2. In **Security Administration** window, perform any of the following procedures:
  - o From the **File** menu, choose **New > AddOperations**.
  - o Press **Ctrl+Shift+O**.
  - o Click **AddOperation**.

The **Operations** window is displayed.

3. Click the parent operation under which you need to add a new operation. For example, **Events**. For information on the default operations, refer to Understanding Default Operations.
4. In the empty field given below the tree, type a name for the operation and click **Add**. The operation is added to the tree under the selected parent node. Repeat this step to add more operations.
5. Click **Ok**.

## 6.8.3.4 Deleting Operations

### To delete an operation

1. In the Application Client, perform any of the following procedures:
  - o From the **Tools** menu, choose **Security Administration**.
  - o Press **Alt+S**.

The **Security Administration** window is displayed.

2. In **Security Administration** window, perform any of the following procedures:
  - o From the **File** menu, choose **New > AddOperations**.
  - o Press **Ctrl+Shift+O**.
  - o Click **AddOperation**.

The **Operations** window is displayed.

3. Click the operation you need to delete.
4. Click **Remove**. To confirm deletion, click **Yes**.

## 6.8.4 Authorization for Security Operations

The security management module of NMS provides an authorized mode of performing the security operations for a group or user. This feature is facilitated by making a configuration in the startup options of security module.

### To enable authorization support

1. Before you start the NMS server, edit the file **NmsProcessesBE.conf** present in <Web NMS Home>/conf directory.
2. Go to **com.adventnet.nms.security.authorization.NmsAuthManager** process.
3. By default the argument **authorization\_for\_security\_administration** is set **false**. Configure this value as **true**.
4. Save the file and then start the NMS server.

On setting the **authorization\_for\_security\_administration** to **true**, the authorization support is enabled for all security operations. Thereby the users will not be able to perform the operations and set permissions (for which they are not authorized to do so) in the Security Administration UI.

### An Example

Here is an example that captures two different scenarios - authorized mode for security operations and unauthorized mode of security operations. On performing this example you will understand the difference between an authorized and unauthorized mode of performing security operations. Follow the steps given below to accomplish the task.

#### Step 1:

Before starting the NMS server, set the **authorization\_for\_security\_administration** argument as **true** in **NmsProcessesBE.conf** file present in <Web NMS Home>/conf directory. This is the authorized mode.

#### Step 2:

Start the NMS server and log in to the client as an administrator with default user ID **root** and password **public**. Invoke the **Security Administrator UI** by choosing **Tools > Security Administration** from the menu bar.

#### Step 3:

Right-click **Groups** node in Security tree and click **AddGroup**. Create a new group **Group1**. Click **Next**. In the Permissions tree hierarchy, enable Security Administration node and then disable Add Group, Remove Group, and Remove Operation operations. A screen shot depicting the configuration is given below. For more information on creating a new group, refer to Adding a New Group.



#### Step 4:

Right-click the **Users** node in Security tree and click **AddUser**. Create a new user '**Group1User**' with password **group**. In the final screen of the wizard, select **Group1** under **Assign Groups for the user** field and click **Finish**. You have now associated the user **Group1User** with the group **Group1**. For more information on creating a new user, refer to Adding a New User.

Click **Finish** and quit the Security Administration UI and the Web NMS client.

#### Step 5:

Log in to the client again with user ID **Group1User** and password **Group**. From the **Tools** menu, choose **Security Administration**. The **Security Administration** window is displayed.

Now try adding a new group. A message **Group1User is not authorized to perform the operation** is displayed.



This occurs because we have disabled this particular user from adding a new group. Similarly, try removing an existing group and removing an existing operation. The same message is displayed.

#### Step 6:

Close the client and shut down the server. Set the **authorization\_for\_security\_administration** argument as **false** in **NmsProcessesBE.conf** file present in <Web NMS Home>/conf directory. This is the unauthorized mode. Now restart the server and log in to the client with user ID **Group1User** and password **Group**. From

**Tools** menu, choose **Security Administration**. The **Security Administration** window is displayed.

Now try adding a new group. You will be able to create the group and no error message is displayed. This is because no authorization support is provided for performing the security operations alone.

## 6.8.5 Security Management - Configurable Parameters

The startup options of the Security Management module can be modified by editing the parameters of **NmsAuthenticationManager** and **NmsAuthManager** processes in the **NmsProcessesBE.conf** file located in <Web NMS Home>/conf directory.



**Note:** If you have configured any of the parameters, ensure to restart the Web NMS Server.

The parameters that can be configured by administrators are listed below. For complete information, follow the links provided for each of the parameters.

- To set the count for maximum allowed unsuccessful login attempts - `maximum_allowed_login_failed_count` in **NmsAuthenticationManager**
- To set the time interval in milliseconds for the security scheduler - `time_interval_for_security_scheduler` in **NmsAuthManager**
- To change the password after the first time logging in - `change_password_for_firstrime_login` in **NmsAuthManager**

## 6.8.6 Security Management: An Example

This example helps you in fulfilling the following hypothetical case.

1. A new group **NMSGroup** is created.
2. The **NMSGroup** has the privilege to do all operations in the following modules.
  - o Events
  - o Topology
  - o Maps
3. The **NMSGroup** does not have the privilege to perform the following operations.
  - o Stop the Web NMS Server
  - o Configure for security
4. A new user **NMSUser** is created.
5. The **NMSUser** is assigned to the **NMSGroup**.
6. The NMS User can view details of **NODE\_0** only in the Application Client.

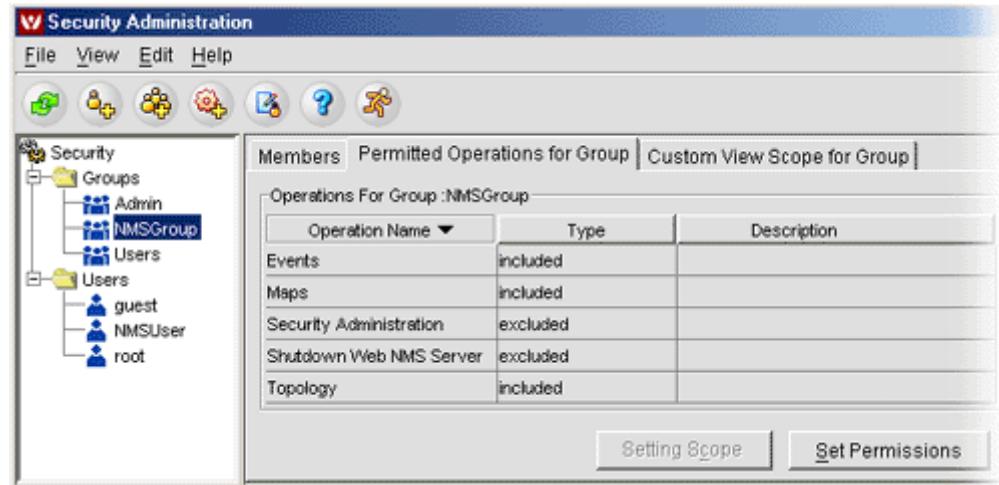
Follow the steps to achieve the above listed criteria.

### Adding the 'NMSGroup' Group

1. In the Application Client, perform any of the following procedures:
    - o From the **Tools** menu, choose **Security Administration**.
    - o Press **Alt+S**.
- The **Security Administration** window is displayed.
2. In **Security Administration** window, from the **File** menu, choose **New > AddGroup**. The **Groups Wizard** is displayed.
  3. Type the group name as **NMSGroup** and click **Next**. The **Operations Tree Root** is displayed. No entries required in this window. We will perform it later.
  4. Click **Finish**. The NMS Group is created and you can view it on the **Security** tree under **Groups**.

### Assigning Operations to 'NMSGroup' Group

5. In the **Security** tree, click **NMSGroup** under **Group**.
6. Click the **Permitted Operations for Group** tab displayed on the right side.
7. Click **Set Permissions**. The **Assign Permissions** window is displayed. The operations tree is empty now as no operations were assigned to this newly added group.
8. Select (**tick**) the check boxes of **Events**, **Topology**, and **Maps**. This selects all the check boxes under these parent operation nodes.
9. Select (**X**) the check boxes of **Shutdown Web NMS Server** and **Security Administration**.
10. Click **Done**.



## Configuring Custom View Scope for 'EMS Test' Group

11. Click the **Custom View Scope for Group** tab.
12. From the **Custom View Scope for Group** drop-down box, choose **Events**.
13. Click **Add AuthorizedScope**. The **Scope Settings** dialog box is displayed.
14. Type the scope name as **EventTest**.
15. From **Name** drop-down box, choose **source**.
16. Type **Value** as **NODE\_0\***.
17. Click **Add**.
18. Click **Ok**.
19. Repeat steps 12 to 18 for other modules, such as **Network Database**, **Alerts**, **Maps**, **Stats Admin**, and **Provisioning** (available in **Custom View Scope Name** drop-down box).

## Adding the 'NMSUser' User

20. From the **File** menu, choose **New > Add NewUser**. The **User Administration** wizard is displayed.
21. Type the user name and password as **NMSUser**.
22. Click **Next**.
23. Click **Next**.
24. From **Assign groups for the user** select **NMSGROUP**.
25. Click **Finish**. All the operations configured for NMSGROUP is now be available to this user.

Now log on to the Application Client with user name and password as **NMSUser**. Only information related to **NODE\_0** is displayed in all modules of the Application Client.

## 6.9 Provisioning

The Provisioning Framework provides parameterized XML provisioning templates, which are created as needed for specific applications. The templates are used for domain-specific provisioning or configuration tasks, e.g. configuring a frame relay interface on a router. The XML-based template provisioning makes building solutions much simpler. Many different provisioning solutions can be built with minimal effort, and often by simply creating and editing XML templates.

These templates are placed in `<Web NMS Home>/provisioningtemplates` directory and in `<Web NMS Home>/examples/provisioning/templates/` directory. Network Administrators can invoke these templates for specific operating needs, from Web NMS Client, through Applet Client or using batch/script files. You can also view the status of the executed provisioning templates and schedule it to be executed at specified time.

- 
- Invoking Provisioning Templates
  - Scheduling and Provisioning Templates
  - Deleting and Reloading Templates
  - Working with ActivityList
  - Setting User Privileges
-

## 6.9.1 Invoking Provisioning Templates

The Provisioning templates that are built according to the application-specific needs can be invoked in three different ways:

- using the Batch/Script files
- using TemplateTesterApplet Client or
- using Web NMS Client

### Using Batch/Script files

#### To invoke provisioning templates using batch/script files

1. Invoke the **OpenTemplate.sh/bat** file located in the *<Web NMS Home>/provisioningtemplates* directory. The **Provisioning** wizard is displayed.
2. Specify the user name, password, port, and mode of connection.
3. Click **Next**. The provisioning templates located in the *<Web NMS Home>/provisioningtemplates* directory are listed.
4. Select the provisioning template and continue specifying values in further screens to accomplish the provisioning.

### Using TemplateTesterApplet Client

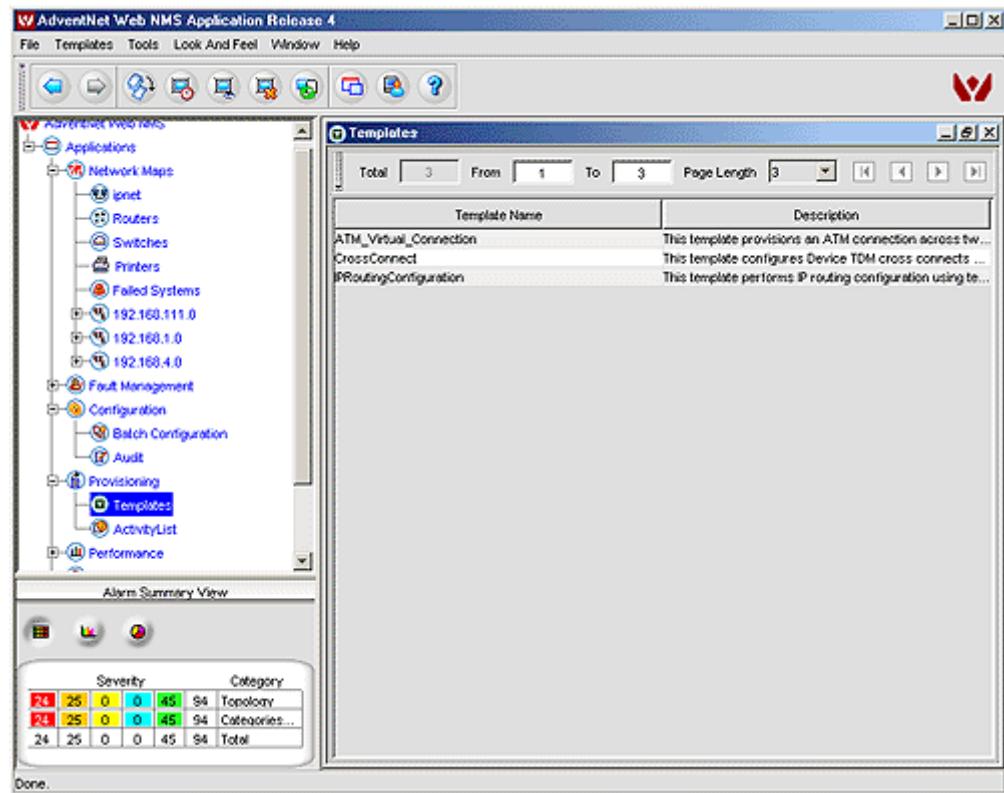
#### To invoke the provisioning templates using TemplateTesterApplet client

1. In the Web browser, type the URL **http://<hostname>:9090/html/TemplateTesterApplet.html** on the address bar and press enter. An applet is instantiated and the Provisioning Authentication page is displayed.
2. Specify appropriate values to provision the template.

### Using Web NMS Client

#### To invoke provisioning templates from Web NMS Client

1. Start the Web NMS Server and Client.
2. In the Client, click the **Provisioning > Templates** node on the left-side tree. The templates available in the *<Web NMS Home>/provisioningtemplates* directory are displayed in the right-side **Templates** panel.



3. Select a template.
4. From the **Templates** menu, choose **Provision** or press **Ctrl+Shift+P** or right-click on the selected template and choose **Provision**.

### Viewing XML Format of the Provisioning Templates

You can also view the XML format of the predefined provisioning templates available in <Web NMS Home>/provisioning/templates directory.

1. In the Template panel, select a template.
2. From the **Templates** menu, choose **View** or press **Ctrl+V** or right-click on the selected template and choose **View**.
3. A window with the provisioning template in XML format is displayed.

## 6.9.2 Scheduling and Provisioning Templates

- Scheduling Templates
- Provisioning Templates

### Scheduling Templates

#### To schedule the execution of templates at specified intervals

1. In the Web NMS Client, click **Provisioning > Templates**.
2. Select a template on the right-side **Template** panel.
3. From the **Templates** menu, choose **Schedule** or press **Ctrl+S** or right-click on the selected template and choose **Schedule**. The provisioning wizard is displayed.
4. Specify appropriate values in the fields available and click **Provision**. The **Provisioning** dialog box is displayed. Specify the date and time when you need the provisioning operation to be executed and click **OK**.

On performing this, the provisioning operation is scheduled at the configured date and time. This information can be viewed in the **ActivityList**.

### Provisioning Templates

#### To provision a particular template for specific operations

1. In the Web NMS Client, click **Provisioning > Templates**.
2. Select a template on the right-side **Template** panel.
3. From the **Templates** menu, choose **Provision** or press **Ctrl+Shift+P** or right-click on the selected template and choose **Provision**. The provisioning wizard is displayed.
4. Specify required values for the fields available.

If you select (enable) the **Show Debug Information** option in the Provisioning wizard, once the task is executed, you can view the debug information of that task. This information provides an insight into the success or failure of an executed provisioning template.

5. You can view the debug information in the Java console if the provisioning template is invoked through the NMS Client, otherwise the same gets displayed in the command prompt screen on invoking the template by running the **OpenTemplate.bat/.sh** file located in the **<Web NMS Home>/provisioningtemplates** directory.
6. Click **Provision** to execute the provisioning operation.

On performing this, a window displaying the result of the provisioning operation is displayed. For more details on the operation, select the Task Name and click **Details**. The **Provisioning - Result Details** dialog box with information on the device name, the configuration status, Rollback Status, Attribute Identifiers, and Device Lists is displayed. The color depicted in the **Device List** determines whether the configuration has failed (red), succeeded (green) or ignored (gray).



**Note:** Even if one task is configured through the corresponding displayed form (of the provisioning template) all the other tasks defined in the same template also get applied during template execution.

## 6.9.3 Deleting and Reloading Templates

- 
- Deleting Templates
  - Reloading Templates
- 

### Deleting Templates

#### To delete a template

1. In the Web NMS Client, click **Provisioning > Templates**.
2. Select a template on the right-side **Template** panel.
3. From the **Templates** menu, choose **Delete** or press **Ctrl+D** or right-click on the selected template and choose **Delete** or from the toolbar click **Delete Selected Template**. A confirmation is asked.
4. Click **Yes** to delete the template.

On performing this, the template which is an XML file is deleted from the *<Web NMS Home>/provisioningtemplates* directory.

### Reloading Templates

#### To reload a template or to reflect the latest changes made to the xml file in the Client

1. In the Web NMS Client, click **Provisioning > Templates**.
2. Select a template on the right-side **Template** panel.
3. From the **Templates** menu, choose **Refresh** or press **F5** or from the toolbar click **Refresh Templates from Server**.

On performing this, the latest changes made to the XML file in the *<Web NMS Home>/provisioningtemplates* directory are reflected in the Template Panel. This can be confirmed by viewing the details of the template.

## 6.9.4 Working with ActivityList

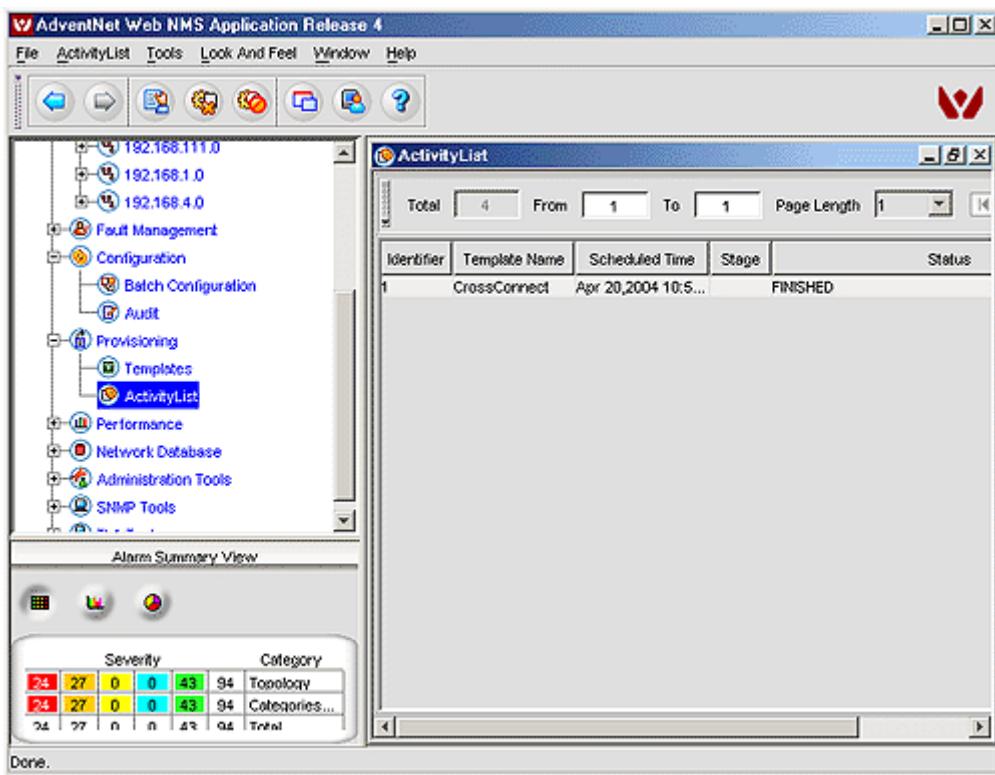
- Viewing ActivityList
- Viewing Result
- Deleting Activity Results
- Stopping a Scheduled Activity
- Reloading the Activity

### Viewing ActivityList

To view the activities associated with the templates

- In the Web NMS Client, click **Provisioning > ActivityList**.

The **ActivityList** panel with the activities associated with the templates is displayed.



**Note:** The activities associated with the templates are displayed, only if there are any predefined activities scheduled or provisioned for a particular template.

## Viewing Result

### To view the result of any specific activity

1. In the Web NMS Client, click **Provisioning > ActivityList**.
2. Select an activity on the right-side **ActivityList** panel.
3. From the **ActivityList** menu, choose **View Result** or press **Ctrl+V** or right-click on the selected template and choose **View Result** or from the toolbar click **Fetch Result**. The **Provisioning Result** window displays the result of the scheduled task.

## Deleting Activity Results

The results pertaining to the activities are stored in the *<Web NMS Home>/provisioningresults* directory.

### To delete the result for a specific activity

1. In the Web NMS Client, click **Provisioning > ActivityList**.
2. Select an activity on the right-side **ActivityList** panel.
3. From the **ActivityList** menu, choose **Delete** or press **Ctrl+D** or right-click on the selected template and choose **Delete** or from the toolbar click **Delete operation from server database**. A confirmation is asked.
4. Click **Yes** to delete the activity result.

## Stopping a Scheduled Activity

### To stop an activity that is currently scheduled or provisioned

1. In the Web NMS Client, click **Provisioning > ActivityList**.
2. On the right-side **ActivityList** panel, select an activity that is yet to be executed.
3. From the **ActivityList** menu, choose **Stop** or press **Ctrl+S** or right-click on the selected template and choose **Stop** or from the toolbar click **Stop scheduled operation**. A confirmation message is displayed.

## Reloading the Activity

### To manually reload the latest activities associated with the templates, from the database

1. In the Web NMS Client, click **Provisioning > ActivityList**.
2. Select an activity on the right-side **ActivityList** panel.
3. From **ActivityList** menu, choose **Refresh** or press **F5** or right-click on the selected template and choose **Refresh**.

### To automatically reload the latest activities associated with the templates, from the database

1. In the Web NMS Client, click **Provisioning > ActivityList**.
2. Select an activity on the right-side **ActivityList** panel.
3. From the **ActivityList** menu, choose **Screen Refresh Interval** or press **Ctrl+I** or right-click on the selected template and choose **Screen Refresh Interval**. The **Provisioning** dialog box is displayed.
4. Use the slider to set the refresh duration in **Hours**, **Minutes**, or **Seconds** after which the activities are to be reloaded from the database.

## 6.9.5 Setting User Privileges

You can prevent a user from accessing certain data in the Web NMS Client and also confine him to viewing and working on only selected Provisioning Templates. This can be achieved using the **Custom View Scope** mechanism of the Security Management. For more information on Custom View Scope, refer to Managing Custom View Scopes topic.

This topic provides an example based on which you can create your own Custom View Scopes.

### Example

This example aims at enabling a set of users belonging to a particular group to access only the Cross Connect Provisioning Template that is available with Web NMS.

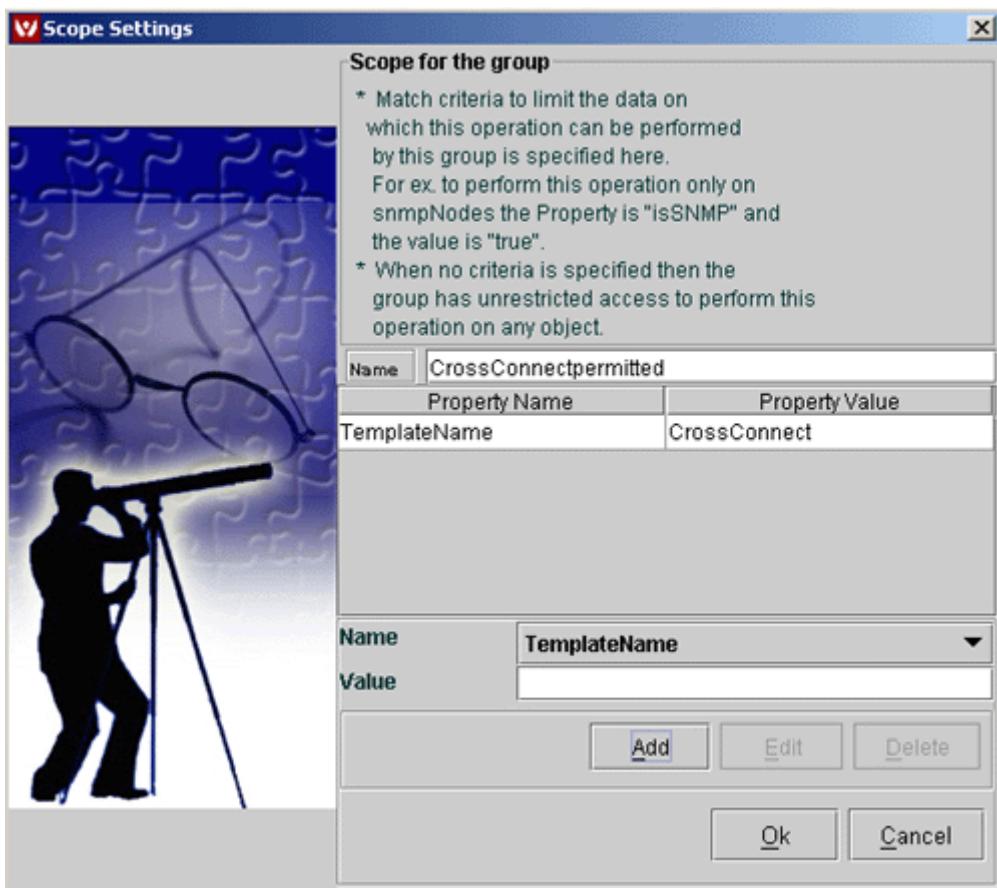
#### Procedure

1. In Web NMS Client, from **Tools** menu, choose **Security Administration**. The **Security Administration** tool is displayed.
2. Add a new user named **user1**.
3. Add a new group named **ProvGroup**.
4. Assign required permissions for the ProvGroup.
5. Assign the new user user1 to the ProvGroup.
6. Set the Scope Criteria.
  - Select the **ProvGroup** on the **Security** tree.
  - Click **Custom View Scope for Group** tab on the right side frame.
  - From **Custom View Scope for Group** drop-down box, choose **Provisioning**.
  - Click **Add AuthorizedScope**. The **Scope Settings** dialog box is displayed. Enter the **Name** as **CrossConnectPermitted**. From **Name** drop-down box, choose the property as **TemplateName** and enter the **Value** as **CrossConnect**. More templates can be specified in the **Value** field as comma-separated values.

**Note:** The value field is case sensitive and wild card characters also cannot be used to specify values in it.

5. The template name comparison is **case sensitive** and hence specify the names in the same case as available.
6. Click **Add**.
7. Click **OK**.

A screen shot depicting the procedure is given below.



7. Log in to the Web NMS Client as **user1**.
8. Click **Provisioning > Templates** on the tree. Only the Cross Connect Provisioning Template is available to this user for execution. If you have set the scope for your own account then refresh the Client to see the permitted list of templates.

## 6.10 Policy Management

A **Policy** refers to a task or set of tasks which are to be executed at a specified time based on a set of specified conditions. The policies can be used to control a variety of network activities, such as automated backups, routing and prioritizing the network traffic, bandwidth allocation, cleaning up the database tables, deleting the failed nodes, etc.

This policy framework enables scalable administration of the Web NMS server and the network elements managed by it. The primary goal of the policy engine is to enable administration of complex functions easily. In Web NMS, policies are used to customize the behavior of the NMS and to provide a framework for adding policies for different network elements.

- 
- Configuring Policies
  - Accessing Policies
  - Viewing Default Policy Details
-

## 6.10.1 Configuring Policies

By default, Web NMS provides a set of policies. For more information on the default policies, refer to Accessing Policies. These policies fall under two categories namely **Periodic** and **Non-periodic** policies. If you have created your own custom policies, use the **Policy Configuration** tool to add them to the existing set of policies.

- Types of Policies
- Invoking the Policy Configuration Tool
- Adding or Modifying a Policy
- Deleting a Policy
- Changing the Policy Color
- Saving Policy Details

### Types of Policies

#### Periodic Policies

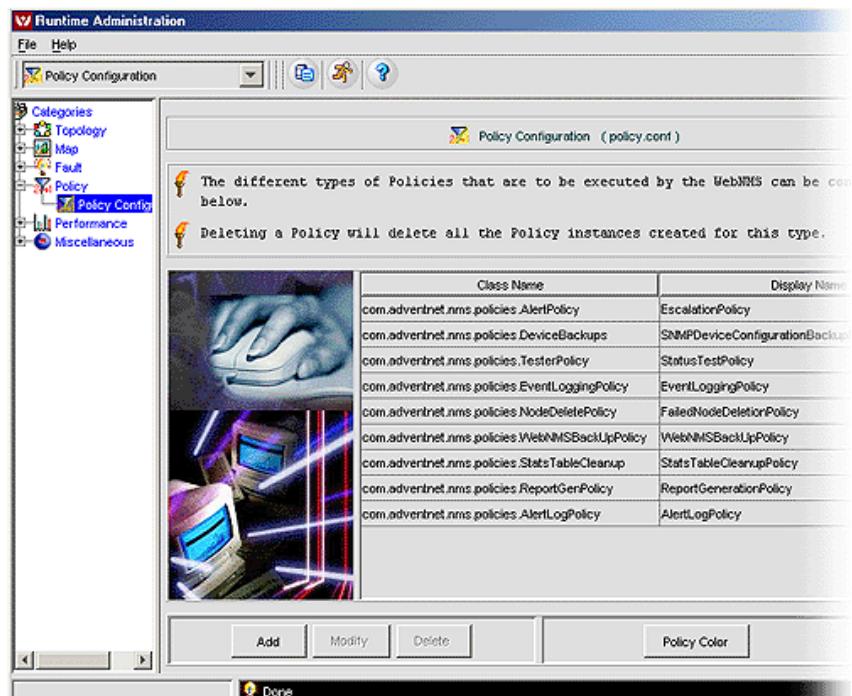
Policies that are triggered periodically by the Server at the specified time interval. By default, the periodic policies are configured to be executed every 10 seconds.

#### Non-periodic Policies

Policies that are executed at the specified time. In this case, there is no fixed time interval. You need to specify the time at which the policy has to be executed. No default value is assigned for non-periodic policies. For information on scheduling non-periodic policy, refer to Scheduling Policies.

### Invoking the Policy Configuration Tool

The Policy Configuration tool helps you to add a new policy to Web NMS or to modify or delete an existing policy. This tool is available with the Runtime Administration tool.



### To invoke the Policy Configuration tool

1. In the Web NMS Client, from the **Tools** menu, choose **Runtime Administration** or press **Alt+R**. The **Runtime Administration** tool is displayed.
2. From the **Categories** tree or drop-down box, choose **Policy > Policy Configuration**. The **Policy Configuration** tool is displayed on the right-side panel which displays all the default and existing policies.

## Adding or Modifying a Policy

Use the Policy Configuration tool to add a new policy to Web NMS. You can also modify the existing and default policies to cater to your network requirements.

### To add a policy

1. In the **Policy Configuration** tool, click **Add**. The **Filter Configuration** dialog box is displayed.
2. In the **Class Name** field, specify the class name to be invoked for executing the policy.
3. In the **Display Name** field, specify a name. On providing this value, the policy is displayed with the configured name in the Client.
4. Click **OK**.

### To modify a policy

1. In the **Policy Configuration** tool, select the policy to be modified.
2. Click **Modify**. The **Filter Configuration** dialog box with the existing Class Name and Display Name values is displayed.
3. Modify the values as required and click **OK**.

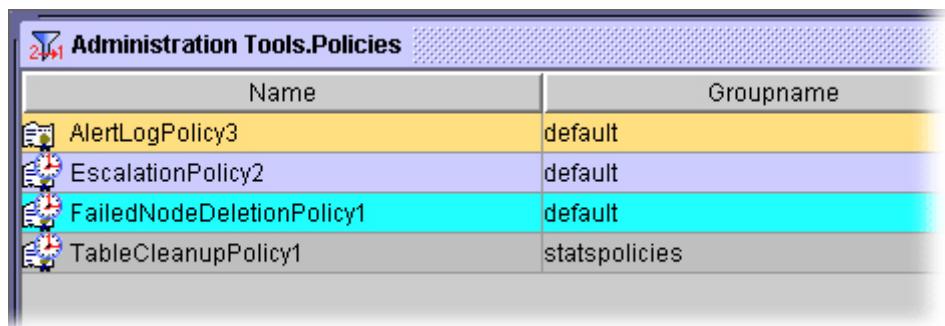
## Deleting a Policy

### To delete a policy

1. In the **Policy Configuration** tool, select the policy to be deleted.
2. Click **Delete**. A confirmation is asked.
3. Click **Yes** to delete the policy.

## Changing the Policy Color

Every instance of policy that is displayed in the **Policies** panel is highlighted with a color. This color signifies the status of the policy. This helps you know the status of a policy instantly. A screen shot depicting few of the colors is given below.



The screenshot shows a Windows application window titled "Administration Tools.Policies". Inside, there is a table with two columns: "Name" and "Groupname". The rows represent different policies, each with a small icon and a unique name. The rows are colored differently, illustrating how policies are highlighted based on their status:

Name	Groupname
AlertLogPolicy3	default
EscalationPolicy2	default
FailedNodeDeletionPolicy1	default
TableCleanupPolicy1	statspolicies

The following are the default colors for policies:

- **Yellow:** A policy that has been stopped from being executed.
- **Green:** A policy that is currently being executed.
- **Cyan:** A policy that has been executed.
- **Grey:** A policy that has been disabled.
- **Orange:** A policy that has been enabled (after it was disabled).

These default color code can be modified based on your requirement.

#### To change policy colors

1. In the **Policy Configuration** tool, click **Policy Color**. The **Policy Color Choose** dialog box with the existing color code is displayed.
2. Click the color to be changed. The **Swatches**, **HSB**, and **RGB** tabs are displayed.
3. Choose the required color.
4. Click **OK**.
5. Click **OK**.

### Saving Policy Changes

After adding, modifying, or deleting a policy, save the configuration to the Server.

#### To save policy changes to Server

1. In the **Policy Configuration** tool, make necessary changes.
2. Click **Apply**.

Once the changes are saved to the server, a confirmation message is displayed on the status bar of the Runtime Administration tool.

## 6.10.2 Accessing Policies

The configured policies can be viewed in the **Administration Tool > Policies** panel. Only policies that are configured to be executed are listed in this view. To view all the policies available for configuration, you need to access the Policy Configuration tool.

Every added policy has certain properties based on which an action is triggered. This section explains how you can view the properties of the default policies available in Web NMS.

- Viewing Policies
- Adding Policies
- Searching Policies
- Updating Policies
- Executing Policies
- Stopping Policies
- Scheduling Policies
- Deleting Policies
- FAQ

---

### Viewing Policies

The existing policies in Web NMS can be viewed through the Client. Only the policies that are configured to be executed are listed in this view.

#### To view policies

1. Open the Web NMS Client.
2. Choose **Administration Tools > Policies**. All the existing policies that are configured to be executed are displayed in the **Policies** panel on the right side.

**Tip:** In the Policies panel, you can identify a non-periodic policy with a clock symbol beside in the policy Name.

### Adding Policies

The policies that are to be executed can be configured in the Web NMS Client.

#### To add policies

1. In the Web NMS Client, click **Administration Tools > Policies**.
2. From the **Policy** menu, choose **Add Policy** or press **Ctrl+P**. The **AddPolicy Details** dialog box is displayed.
3. From the **Select Policy** drop-down box, select the policy that you need to configure for execution.
4. Click **Add**. The **Object Details** dialog box is displayed. For information on each of the fields (for different default policies), refer to Viewing Default Policy Details.

On performing this, the policy is displayed in the **Policies** panel. Now you can proceed to perform other operations, such as executing, updating, stopping, and scheduling the policy.

## Searching Policies

All policies configured to be executed are displayed in the **Policies** panel. When there are more number of policies displayed, use the **Search** option to locate a specific policy.

### To search policies

1. In the Web NMS Client, click **Administration Tools > Policies**.
2. From the **Policy** menu, choose **Search**, or press **Ctrl+F** or from the toolbar click **Find**. The **Search Dialog** is displayed.
3. Specify the match criteria and click **Execute Query**. The policies matching your criteria are displayed in the **Policies** panel.
4. To view all the policies again, in the **Search Dialog**, click **Select all Policies**.

## Updating Policies

After configuring a policy for execution, you can change its properties any time, if need arises. For example, to disable the policy, follow the procedure given below and change the value of 'status' to 'Disabled'.

### To update a policy

1. In the Web NMS Client, click **Administration Tools > Policies**.
2. In the **Policies** panel displayed on the right side, select the policy to be updated.
3. From the **Edit** menu, choose **Update Policy** or press **Ctrl+U** or right-click the policy and choose **Update Policy**. The **Object Details** dialog box is displayed. For information on each of the fields (for different default policies), refer to Viewing Default Policy Details.

## Executing Policies

### To execute a policy

1. In the Web NMS Client, click **Administration Tools > Policies**.
2. In the **Policies** panel displayed on the right side, select the policy to be executed.
3. From the **Edit** menu, choose **Execute Policy** or press **Ctrl+X** or right-click the policy and choose **Execute Policy**.

On performing this procedure, if the policy execution has started, the policy is depicted in cyan (default color code) and if it has completed, the policy is depicted in green (default color code). For more information on the color codes, refer to Changing the Policy Color.

For information on the outcome of executing default policies, refer to Viewing Default Policy Details.

## Stopping Policies

### To stop a policy that is currently being executed

1. In the Web NMS Client, click **Administration Tools > Policies**.
2. In the **Policies** panel displayed on the right side, select the policy to be stopped.
3. From the **Edit** menu, choose **Stop Policy** or press **Ctrl+T** or right-click the policy and choose **Stop Policy**.

The policy is stopped from being executed and the color code changes to yellow (default color code).

## Scheduling Policies

This section explains how you can schedule the day/date/time when a non-periodic policy needs to be executed.

To schedule a policy

1. In the Web NMS Client, click **Administration Tools > Policies**.
2. In the **Policies** panel displayed on the right side, select the policy to be scheduled.
3. From the **Edit** menu, choose **Schedule Policy** or press **Ctrl+H** or right-click the policy and choose **Schedule Policy**. The **Policy Scheduler** is displayed. **Note:** This option is available only if the policy is non-periodic.

There are two modes of scheduling: **Dates** and **Days** scheduling.

### Dates scheduling

By default, the **Dates** option is selected.

- **Select Dates for scheduling policy:** Displays all the dates of a month (from 1 to 31)
- **Select the Scheduling Hours:** Displays hours of a day (0:00 to 23:00). This panel is enabled only if at least a date is specified.

To schedule, click the date or the time (shows a tick symbol on selection). You have options to select all the dates and hours or specific dates and hours.

To schedule specific dates, select a date and the Hour(s). Repeat the same procedure.

**Example 1:** To schedule a policy on the 1st and 10th day of the month and at specific hours

1. In **Select Dates for scheduling policy**, select **Specific** and click **1**.
2. In **Select the Scheduling Hours**, select **Specific** and click the hour(s).
3. In **Select Dates for scheduling policy**, select **10**.
4. In **Select the Scheduling Hours**, select the hour(s).
5. Click **OK**.

**Example 2:** To schedule a policy at 1, 10, and 22 hours on 2nd of the month

1. In **Select Dates for scheduling policy**, select **2**.
2. In **Select the Scheduling Hours**, select **1, 10, and 22**.

Let us assume that you have configured a Date-wise scheduling of a policy for the 5th and 20th hour on the 31st day of every month. As the month of February has only 28 or 29 days, the same policy is scheduled on the 5th hour on 1st of March.

After selecting a date/hour, when you need to deselect it, click the date/hour (with tick) again. The selection is cleared.

## Days scheduling

Click the **Days** option to schedule the policy based on days in a week and hours in a day.

- **Select Days for scheduling policy:** Displays all the days in a month (from 1 to 31)
- **Select the Scheduling Hours:** Displays hours of a day (0:00 to 23:00). This panel is enabled only if at least a day is specified.

To schedule, click the day or the time (shows a tick symbol on selection). You have options to select all the days and hours or specific days and hours.

4. To clear all the configurations that you have made in the **Policy Scheduler**, click **Reset**.
5. Click **OK**.

On performing this procedure, the policy is executed based on the scheduled date/day/time. If you have configured both the date-wise and day-wise scheduling, the configurations that you make finally are effected.

## Deleting Policies

### To delete a configured policy

1. In the Web NMS Client, click **Administration Tools > Policies**.
2. In the **Policies** panel displayed on the right side, select the policy to be deleted.
3. From the **Edit** menu, choose **Delete Policy** or press **Ctrl+C** or right-click the policy and choose **Delete Policy**. The **Policy Scheduler** is displayed.

## FAQ

---

1. **If I schedule a policy on 31st of every month and if a month does not have 31, what is the result?**

If you schedule a policy on 31st of every month, then the policy will be executed only for the months which contain the date 31st. For example, if you have scheduled policy on 31st of every month starting from January, then the policy will be executed on January 31. For February, it will not be executed, since it does not have 31. Again on March 31, the policy will be executed and so on.

2. **Periodic policies are executed once they are added; whereas in case of non-periodic policies, it is not so. Why?**

This is because a default period (10 seconds) is set for periodic policies. So, periodic policies are executed automatically.

On the other hand, no default period or time can be specified for non-periodic policies. You explicitly need to schedule the policy using the **Policy Scheduler**. Otherwise, it will not be executed.

3. **Can non-periodic policy be executed at time schedules of hour:minutes?**

No. Non-periodic policies cannot be executed like that. It can be executed to the precision of hours only and not hours:minutes. For example, it can be executed at 11:00, 12:00, etc. and not at 11:30, 12:15, etc.

### 6.10.3 Viewing Default Policy Details

By default, Web NMS provides a set of default policies. This section explains the purpose of those policies and the properties to be specified in them for execution.

---

- Alert or Escalation Policy
  - SNMP Device Configuration Backup Policy
  - Status Test Policy
  - Event Logging Policy
  - Failed Node Deletion Policy
  - Web NMS Backup Policy
  - Statistics Table Cleanup Policy
  - Report Generation Policy
  - Alert Log Policy
-

## Alert or Escalation Policy

**Alert Policy**, also known as Escalation Policy, is an example of periodic policy. This policy fetches alarms from the database and checks whether any alarm is in the same state (without any change in severity) for a specified period of time (specified by the user). If so, it performs the specified action configured by the administrator in this policy. Alert Policy, being periodic, is automatically scheduled by the Policy Manager.

### On Execution

On executing this policy, an action is instigated (based on the type configured). For example, if an action type **Send Email Action** is configured, executing this policy results in sending an e-mail to the recipient's address. Similarly, for all the other action types, a particular action is triggered on executing this policy.

### Properties

For information on updating the policy properties, refer to Updating Policies.

AdventNet Inc.

The following table explains each of the fields (properties) in the **Escalation Policy Object Properties** dialog box.

Property	Description
<b>Policy Name</b>	A non-editable field that displays the name of the instance of the policy. It helps to identify the policy while managing the list of policies.
<b>Group Name</b>	Displays the default group name. The default name is <b>Escalation Policy</b> . Edit this field to change the group name.
<b>Status</b>	Specify whether the policy is Enabled or Disabled. The policy can be executed only if the status is Enabled.
<b>Periodicity</b>	Specify the interval (in seconds) between two successive execution of the policy. Default value is 10 seconds.
<b>Severity</b>	It specifies the severity of an alarm. That is, the severity which does not change for a particular alarm until the time specified by the use (the corresponding action to be executed for the alarm is covered in the match criteria).
<b>Category</b>	Specify the category which serves as a match criterion.
<b>Alert Group Name</b>	Specify the name of the alert group (if created through a custom view).
<b>Source</b>	Specify the name of the source whose alerts are to be picked which serves as a match criterion for picking alerts.
<b>Entity</b>	Specify the name of the interface through which the source whose alerts are to be picked, communicates (serves as a match criterion).
<b>Owners's List</b>	Specify the e-mail IDs of only the owners to whom information about the picked alerts is to be intimated (e-mailed). Applicable to 'Send E-mail Action'.
<b>Action Time (in secs)</b>	Specify the maximum time limit for an alarm to remain in a particular state. If an alarm remains in the same state for more than the specified period, then an action is triggered.

## Action Types

The actions that can be triggered on executing the Escalation Policy are:

- Suppress Action
- Send Trap Action
- Send E-mail Action
- Custom Filter
- Run Command Action
- Set Severity

### Suppress Action

This action suppresses alarms matching a particular criterion, either altogether, or multiple alarms of the same type within a given interval. On the occurrence of an alarm, you can suppress all of them, that match a particular filter.

### To suppress alarms

1. In Escalation Policy dialog box, in **Action Type** panel, select **SUPPRESS ACTION**.
2. In the **Action details** panel, specify the action name in **SUPPRESS ACTION NAME**.
3. To suppress all the events and alarms, select **Yes** in **SUPPRESS ALL** field.

To suppress multiple alarms for a given interval, select **No**. The **SUPPRESS INTERVAL** field is enabled. Specify the interval in seconds. On specifying the **SUPPRESS INTERVAL**, the first alarm is allowed and all subsequent alarms are suppressed for the given interval. After the suppress interval has elapsed, the first alarm is allowed again and the subsequent alarms are suppressed and so on.

### Send Trap Action

This action sends SNMP v1 or v2c traps for the alarms matching the specified criteria.

### To send traps

1. In Escalation Policy dialog box, in **Action Type** panel, select **SEND TRAP ACTION**.
2. In the **Action details** panel, specify appropriate values.
  - **Send Trap Action Name:** Specify a name for the trap action.
  - **Trap Destination:** Specify the host to which the trap has to be sent.
  - **Destination Port:** Specify the destination host port to which the trap has to be sent.
  - **Trap Community:** Specify the community string to be set for the generated trap.
  - **Enterprise:** Specify the enterprise OID of the trap.
  - **Generic Type:** Specify the generic type number to be used for the trap.
  - **Specific Type:** Specify the type number to be used for the trap.
  - **SysUpTime:** Specify the sysuptime value to be used in the trap.
3. You can also set variable bindings to the trap. To add a variable binding, click **Add**. Specify the **OID Value**, **SNMP Type**, and **Set Value**. Click **Update**.

### Send E-mail Action

This action sends an e-mail on receiving an alarm of a specific kind (specified in the filter match criteria).

### To send e-mail

1. In Escalation Policy dialog box, in **Action Type** panel, select **SEND E-MAIL ACTION**.
2. In the **Action Details** panel, specify appropriate values.
  - **Send Email Action Name:** Specify a name for the e-mail action.
  - **User Name:** Specify the user name using which the mail server will authenticate you to send the e-mail.
  - **Password:** Specify the password using which the mail server will authenticate you to send the e-mail.
  - **SMTP Server:** Specify the SMTP server name.

- **Recipient's Address:** Specify the destination address to which the e-mail should be sent. Example: mail@action.com
- **Sender's Address:** Specify the sender's address from which the e-mail is being sent.
- **Subject:** Specify the subject of the mail.
- **Message:** Specify the message to be sent in the mail.
- **File Attachment:** Specify the location of file to be attached in the mail.

### Custom Filter

Apart from the actions provided here, you can create your own custom filter and define rules for processing the alarms. To use custom filters, write your own filter class in JAVA. The custom filters that you implement must be compiled and placed in the CLASSPATH of the Web NMS Java Virtual Machine.

#### To use custom filters

1. In Escalation Policy dialog box, in **Action Type** panel, select **Custom filter**.
2. In the **Action Details** panel, specify the appropriate values.
  - **Custom Filter Action Name:** Specify a name for the custom filter.
  - **Custom Filter Class Name:** Specify the custom filter class name. Example: you can specify the fully qualified name  
***com.adventnet.nms.CustomFilter***

### Run Command Action

This action triggers a specific command when an alarm is received.

#### To run a command

1. In Escalation Policy dialog box, in **Action Type** panel, select **Run command action**.
2. In the **Action Details** panel, specify the appropriate values.
  - **Run Command Action Name:** Specify a name for the run command action.
  - **Run Command:** Specify the command string to be executed. The command string should be a machine executable program on the server that does not require a shell, i.e., it cannot be a batch or shell file. To use shell scripts or commands, you must invoke the shell as a part of the command string. The command string should be specified with the full path of the shell, where the server has been started.
  - **Command Results:** To append the output or errors from the command to the event message text, choose **Append Output** or **Append Errors** respectively. Choosing either of the options results in the command being run synchronously in the main event processing thread. This delays all alarms, following the alarm being processed, until the command execution completes or is terminated by the timeout option.
  - **Abort After:** Specify the *timeout* for the command. After the time specified in this field, the command execution is stopped. This is important, if you are appending the output or errors, since all alarm processing is held up by the command execution.

As part of the command string, you can specify alarm and associated trap object attributes as tokens to enable the user to pass event and associated trap information to the command.

## Set Severity

This action escalates or de-escalates the severity of an alarm.

### To set severity

1. In Escalation Policy dialog box, in **Action Type** panel, select **Set severity**.
2. In the **Action Details** panel, specify the appropriate values.
  - **Action Name:** Specify a name for the set severity action.
  - **Set Severity:** Choose the severity from this drop-down box.
  - **Message:** A default message is available. Edit this field to specify the required message.

## SNMP Device Configuration Backup Policy

This backs up SNMP devices and creates backup configuration data for the device. This data can later be used to restore a device, whose configuration has been lost. This is primarily useful for devices configured via SNMP, but can also be used to record data for auditing network activity (for example, what is being configured on network devices and when).

The backup is for a MIB sub-tree on the device. For example, interfaces group on a device, or the entire contents of any standard or enterprise MIB (for example, all variables in the bridge MIB). If you need to collect data on multiple MIB sub-trees, use multiple policies on the same set of devices.

The data is stored in a dated file in the specified directory (default is <DEVICE\_BACKUPS>). The number of files that are created depends on the number of devices and the period between collections.

### On Execution

When you execute this policy, a backup of the configuration data of the SNMP devices starts. This data can later be used to restore a device, whose configuration has been lost.

### Properties

For information on updating the policy properties, refer to Updating Policies.

The following table explains each of the fields (properties) in the **SNMP Device Configuration Backup Object Properties** dialog box.

Property	Description
<b>groupName</b>	Displays the default group name. This field can later be used to query for the matching policies and to organize the different policies.
<b>Maximum Data (variables)</b>	Specify the maximum amount of data (variables) to be collected from a device. Some devices store a lot of MIB data to avoid collecting too much data when the OID is configured erroneously. The default value of 1000 should meet most needs, but change it if you expect more than 1000 variables to be collected.
<b>MIBs to be Loaded</b>	Specify MIB to be loaded in the server before taking backups. This allows using variable names instead of typing the entire object identifiers when specifying what to back up. Use the path relative to the <Web NMS Home> directory, or the entire URL, e.g. mibs/Printer-MIB, when specifying the printer MIB in the mibs directory.

Property	Description
<b>Backups Directory</b>	Specify the location where the files with backup data should be saved. This directory is created only if configured. The default directory is <DEVICE_BACKUP> created under the <Web NMS Home> directory.
<b>Device Type</b>	Specify the prefix of the device types you need to back up. For example, specifying <b>bay</b> backs up the chosen MIB tree for all devices whose type begins with <b>bay</b> .
<b>MIB Sub-Tree to Backup</b>	This is the object identifier for the sub-tree to collect data. You can use the label of the MIB node if the MIB is loaded, e.g. interfaces for the interfaces group. Otherwise, use the numeric OID, e.g. .1.3.6.1.2.1.2 for the interfaces group.
<b>period ( in seconds )</b>	This specifies how often to back up the data, in seconds. The default value is once a day, which can be changed if required.
<b>name</b>	A non-editable field that displays the name of the policy - <b>SNMPDeviceConfigurationBackupPolicy</b> .
<b>status</b>	This determines if this policy is Enabled or Disabled. The policy can be executed only if the status is Enabled.

## Status Test Policy

Status Test Policy can be used to change the tester class for a particular object at runtime for a specific match criterion.

### On Execution

This policy fetches the managed objects from the database which matches the given criteria and changes the tester class of the managed object with the specified one in the Status Test Policy properties form.

### Properties

For information on updating the policy properties, refer to Updating Policies.

The following table explains the fields (properties) in the **Status Test Policy Object Properties** dialog box.

Property	Description
<b>Policy Name</b>	A non-editable field that displays the name of the status test policy.
<b>Group Name</b>	Specify the group with which the policy is associated.
<b>Type</b>	Specify the type of the managed object. Examples: Network, snmp-node, Interface, and LinkObject.
<b>Change tester to</b>	Choose the max, ping, snmpping, or usertest to which the tester is to be changed.
<b>Tester Class</b>	Specify the name of the new tester class to be executed.
<b>Status</b>	Specify if the policy is Enabled or Disabled. The policy can be executed only if the status is Enabled.
<b>Community</b>	Specify the community - public or private. This is used to choose the managed object for changing the tester class.
<b>Parent Network</b>	Specify the parentnet of the managed object, whose testerclass has to be changed.

## Event Logging Policy

Event Logging Policy is used to log the events generated for a particular period of time in a file. It is a periodic policy.

### On Execution

By default, the Event Logging policy's period over which it has to be executed, is set as one day. When this policy is executed, the events that are recorded over a certain period of time are read from the events database and stored in a file. For example, if 1000 events are read during a certain period, the next time, when the policy is executed, the next set of events are read (from the 1001st event).

### Properties

For information on updating the policy properties, refer to Updating Policies.

The following table explains each of the fields (properties) in the **Event Logging Policy Object Properties** dialog box.

Property	Description
<b>Policy Name</b>	A non-editable field that displays the name of the policy.
<b>Group Name</b>	Specify the name of the group to which the policy belongs. If default is specified, the policy does not belong to any group. You can execute different policies at the same time by associating them with a common group name.
<b>Status</b>	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when its status is Enabled.
<b>Period</b>	Specify the period over which the policy is to be executed. By default, it is set as one day, i.e. 86400 seconds. For the specified period, the policy fetches event's data from the database and stores it in a file.
<b>Event's Directory</b>	Specify the directory in which the file containing the events generated for that particular period is to be stored.

## Failed Node Deletion Policy

Failed Node Deletion Policy allows you to delete the nodes in the database with **Major** and **Critical** status that exist for more than 7 days (by default) in the database. Such nodes are deleted, provided the nodes have only one interface. Nodes with multiple interfaces remain in the database.

### On Execution

When you execute this policy, all the nodes with **Major** and **Critical** status available in the database for more than seven days are deleted. Such nodes are deleted only if they have only one interface.

### Properties

For information on updating the policy properties, refer to Updating Policies.

The following table explains each of the fields (properties) in the **Failed Node Deletion Policy Object Properties** dialog box.

Property	Description
Delete After (days)	Specify how long the node can exist in the database (after which it is deleted on executing this policy). The default value is 7 days.
Period	Specify (in seconds) how often to back up the data. The default value is once a day.
groupName	Specify the name of the group to which the policy belongs. If default is specified, the policy does not belong to any group. You can execute different policies at the same time by associating them with a common group name.
Status	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when its status is Enabled.
name	A non-editable field that denotes the name of the policy - <b>FailedNodeDeletionPolicy</b> .

## Web NMS Backup Policy

Web NMS provides backup facility, for taking backups of the Web NMS system. Apart from this, backups can be started as policies, which can be configured during runtime. The load on the server is reduced by running Web NMS backup as a policy service, than running backup as a separate process.

### On Execution

On execution, this policy enables Web NMS to take its system backups. The running of Web NMS backup as a policy reduces the load on the server.

### Properties

For information on updating the policy properties, refer to Updating Policies.

The following table explains the fields (properties) in the **Web NMS Backup Policy Object Properties** dialog box.

Property	Description
Status	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when its status is Enabled.
BackUpClassNames	Specify the class name implementing <b>com.adventnet.nms.startnms.BackUpInterface</b> with the package structure. Multiple class names can also be specified.
name	A non-editable field that displays the name of the backup policy.
groupname	Specify the name of the group to which the policy belongs. If default is specified, the policy does not belong to any group. You can execute different policies at the same time by associating them with a common group name.

## Statistics Table Cleanup Policy

The Statistics Table Cleanup policy allows the cleanup of statistical data from the database. This is necessary to ensure that the database does not outgrow as data is collected each day. You can decide how many days' data has to be saved using this policy. This policy deletes the data that is older than the specified number of days. The hour of execution of this policy can also be specified.

### On Execution

On executing this policy, the statistical data is cleaned up in the database. This saves your time from cleaning up unwanted data manually.

### Properties

For information on updating the policy properties, refer to Updating Policies.

The following table explains the fields (properties) in the **Statistics Table Cleanup Policy Object Properties** dialog box.

Property	Description
<b>Delete data after (days)</b>	Specify how long to store the data in the database, before it is deleted. The default value is seven days.
<b>status</b>	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when its status is Enabled.
<b>name</b>	A non-editable field that displays the name of the policy - <b>StatsTableCleanupPolicy</b> .
<b>Period</b>	A non-editable field that specifies the interval (default interval - 3600 seconds) at which the policy checks whether it is time for cleanup.
<b>groupName</b>	Specify the name of the group to which the policy belongs. If default is specified, the policy does not belong to any group. You can execute different policies at the same time by associating them with a common group name.
<b>Table Name</b>	Specify the name of the table that stores the statistical data. By default, the name is STATSDATA%, unless you have changed the data collection parameters. If you have specified your own table name in the data collection parameters, that table name should be specified in this field. In fact, any table which stores the time in the time field can be specified. However, this is intended only for the statistics tables.
<b>Cleanup Hour (0-23)</b>	Specify (hour of the day) when to clean up the statistics. It can happen at any point of time during the specified hour which cannot be controlled. The default value is 0, i.e., done between 12 at midnight and 1 a.m.

## Report Generation Policy

The Report generation policy generates report based on the data collected at runtime. It is a non-periodic policy. You can specify the time of execution of the policy during runtime.

### Properties

For information on updating the policy properties, refer to Updating Policies.

The following table explains each of the fields (properties) in the **Report Generation Policy Object Properties** dialog box.

Property	Description
<b>Status</b>	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when its status is Enabled.
<b>Name</b>	A non-editable field that displays the name of the report generation policy.
<b>ReportGenClassName</b>	Specify the class name implementing <b>com.adventnet.nms.poll.Reporter</b> , with the package structure. Multiple class names can also be specified.
<b>groupName</b>	Specify the name of the group to which the report generation policy belongs.

## Alert Log Policy

The Alert Log Policy is used to control the number of alarms in the database. You can specify the alarm count, and if the number of alarms exceeds the specified count, the older alarms are deleted from the database. This is done to maintain the specified count in the database.

### On Execution

On executing this policy, you can delete the older alarms from the database which had surpassed the specified alarm count value. Thereby, you can control the alarm count in the database.

### Properties

For information on updating the policy properties, refer to Updating Policies.

The following table explains each of the fields (properties) in the **Alert Log Policy Object Properties** dialog box.

Property	Description
<b>alertLogsize</b>	Specify the count to control the number of alarms in the database. If the number of alarms goes above the specified value, the older alarms are deleted from the database.
<b>Status</b>	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when its status is Enabled.
<b>name</b>	A non-editable field that displays the name of the Alert Log Policy.
<b>groupname</b>	Specify the name of the group with which the Alert Log Policy is associated.

## 6.11 Administration Tools

This topic discusses the administration tools that are available with the Web NMS.

---

- **Runtime Administration**

An easy-to-use tool that helps in administering various modules of Web NMS at runtime. Making configurations at runtime using this tool avoids the hassles of restarting the Web NMS Server every time you make a configuration.

- **SNMPv3 Security Configuration**

A tool to configure the SNMPv3 parameters used by Web NMS for managing and monitoring the network using SNMPv3 protocol. This tool has a Configuration wizard, which helps you to add the security parameters into the Web NMS database.

- **Status Viewer**

A tool that provides real-time information about the Web NMS Server, the network, the number of objects/events, and memory usage. You can use this tool from a remote machine where Web NMS Client is installed.

- **Trap Parser**

A tool to generate Events from the received SNMP traps. It facilitates in making the notifications readable to the user.

- **Event Parser**

A tool that helps to refine the message conveyed by the Events. It converts Events, such as Threshold Events and Status Poll Events into a readable format.

- **Event Filter**

A tool to perform automatic actions, such as sending an e-mail, suppressing the event, and generate traps, on the occurrence of an event.

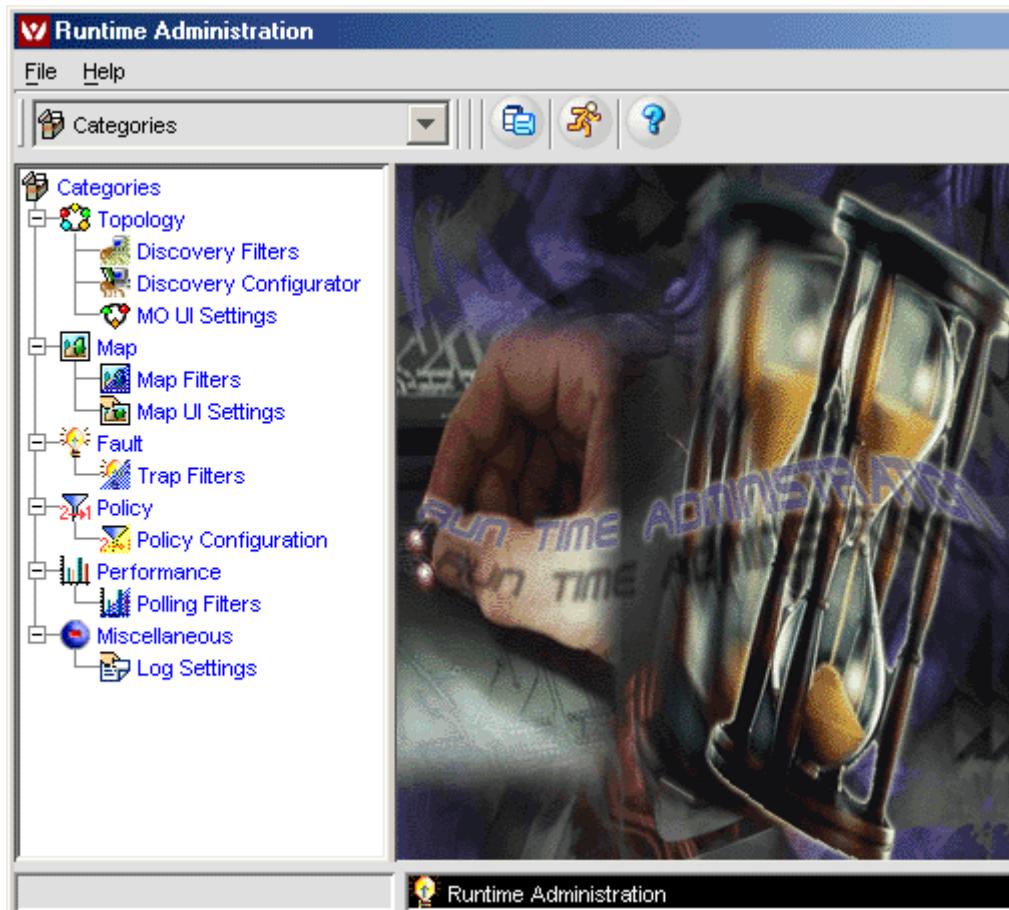
- **Alert Filter**

A tool to filter and modify the properties of the incoming alert/alarm. When an alarm is received by Web NMS, it is passed through the Alert Filters, if the match criteria match with the properties of the alert.

---

## 6.11.1 Runtime Administration

The Runtime Administration tool is an easy-to-use tool that helps in administering various modules of Web NMS at runtime. Making configurations at runtime using this tool avoids the hassles of restarting the Web NMS Server every time you make a configuration.



### Invoking Runtime Administration Tool

#### To open the Runtime Administration Tool

1. Open the Web NMS Client.
2. From the **Tools** menu, choose **Runtime Administration** or press **Alt+R**. The **Runtime Administration** tool is displayed.
3. Choose the required module's tool from the **Categories** drop-down box or tree.

### Modules

Various Administrative tools that you can use in this **Runtime Administration** tool are:

- Discovery Configurator
- MO UI Settings
- Map UI Settings
- Policy Configuration
- Log Settings

Other tools (apart from the above) in this UI are Developer tools, such as Discovery Filter, Map Filter, Trap Filter, and Polling Filter. If you are looking for information on these tools, refer to the Developer Guide.

## 6.11.2 SNMPv3 Security Configuration

- Invoking SNMP V3 Security Tool
- Configuring SNMPv3 Security Parameters

SNMPv3 information is used by Web NMS for managing and monitoring the network using SNMPv3 protocol. Web NMS maintains five Database Tables to configure SNMPv3 parameters. Out of these five tables, four are single column tables. Single column tables contain data of the **Hosts**, **Ports**, **Engine Names** and **User Names** (each value displayed on a different table).

The fifth table contains the complete SNMP v3 configuration information, which includes a combination of **Host Name**, **Port Number**, **User Name** and the **Security parameters** or **Engine name**, **User Name** and **Security parameters**. The Host Name, Port Number, User Name, and the Engine Name data to be added to the SNMPv3 configuration table (fifth table) are taken from these single column tables. The user gives the security parameters for each SNMPv3 configuration.

The **SNMP V3 Security** tool in Web NMS can be used to configure SNMPv3 security parameters.

### Invoking SNMP V3 Security Tool

#### To invoke SNMPv3 Security Tool from Launcher

1. Invoke the **WebNMSLauncher.bat/sh** file located in the <Web NMS Home> directory. The **Web NMS Launcher** is displayed.
2. Double-click **Administration Tools** or right-click **Administration Tools** and choose **Open**.
3. Double-click **SNMP V3 Security** or right-click **SNMP V3 Security** and choose **Run**. The **SNMP V3 Security** tool is displayed.

#### To invoke SNMPv3 Security Tool from Client

1. Open the Web NMS Client.
2. Choose **SNMP Tools > SNMP V3 Security** from the tree. The **SNMP V3 Security** tool is displayed on the right-side panel.

### Configuring SNMPv3 Security Parameters

#### To configure SNMPv3 Security Parameters

1. Invoke the **SNMP V3 Security** tool. For more information, refer to the Invoking SNMP V3 Security Tool section.
2. Specify appropriate values in the fields. Explanation on each of the fields is given in the table.

Field	Significance
Target Host	Enter the host name in this field.
Target Port	Enter the port where SNMP Agent runs.
UserName	Enter the security user name.
Security Level	Choose the security level from this combo box such as, noAuth,noPriv; Auth,noPriv; Auth,Priv.
Priv Protocol	Displays the Privacy Protocol name.
Auth Protocol	Select the authentication protocol from this combo box.
Auth Password	Enter the authentication password in this field.
Priv Password	Enter the privacy password in this field.

3. Click **Add Entry**.
4. To delete one or more entries added, click **Delete Entry**.

### 6.11.3 Status Viewer

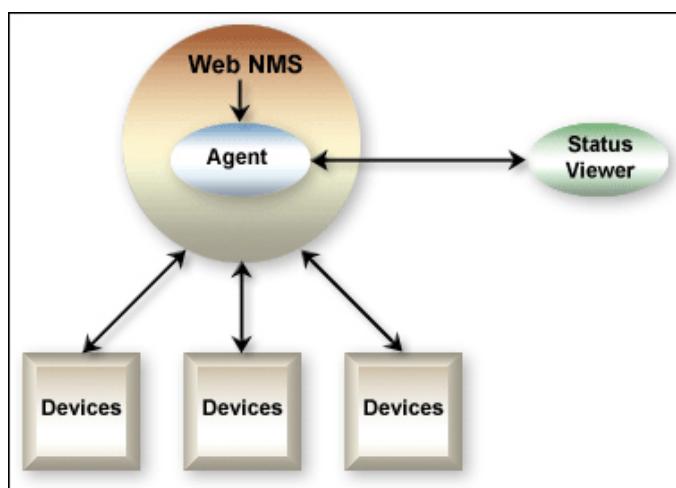
- Overview
- About Status Viewer Tool
- Using the Status Viewer Tool

#### Overview

As a Web NMS Administrator, you require to monitor the status of Web NMS Server which includes:

1. Total memory
2. Free memory
3. Start time
4. Up time
5. Number of nodes managed
6. Number of events generated

Also Web NMS Server requires time-to-time configurations based on your network requirements. This kind of monitoring and configuring can be done on Web NMS from a remote system on the network. Web NMS facilitates this with the help of an built-in agent called **JMX Agent**.



Whenever Web NMS Server is required to be monitored or configured, a request is sent to the **JMX Agent** (labeled as **Agent** in the above image). The JMX agent retrieves the data from Web NMS Server and sends it to the **Status Viewer**.

#### About Status Viewer Tool

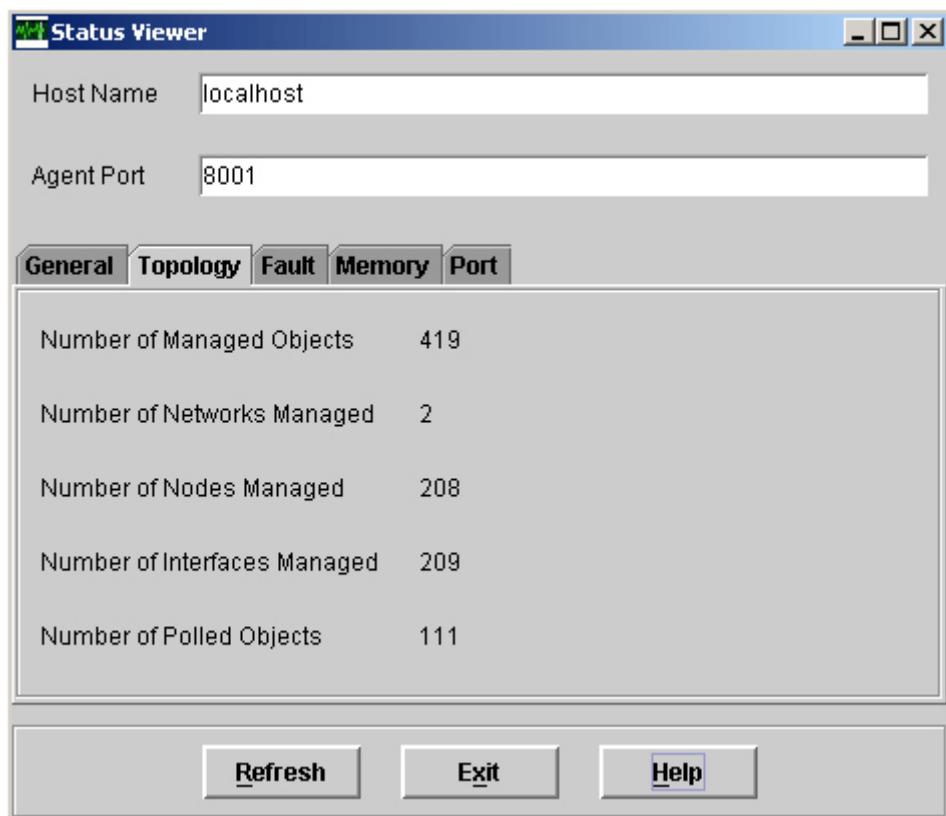
The Status Viewer tool

- Displays the status of Web NMS Server with respect to Topology, Fault, Memory, and Port details.
- Facilitates in monitoring the Server's status and performance.
- Provides real-time information about the Web NMS Server, the network, the number of objects/events and Memory usage.
- Simplifies and centralizes all the day-to-day Server management tasks while providing access to system administration.
- Can be used from a remote machine where Web NMS Client is installed.

## Using Status Viewer Tool

### To open the Status Viewer Tool

1. Invoke the script **WebNMSLauncher.bat/sh** located in the <Web NMS Home> directory. The **Web NMS Launcher** is displayed.
2. Double-click **Administration Tools** or right-click **Administration Tools** and choose **Open**.
3. Double-click **Status Viewer** or right-click **Status Viewer** and choose **Run**. The **Status Viewer** tool is displayed. Ensure that the Web NMS Server is running to view its status.



4. To view latest information, click **Refresh**.

## 6.12 General Administration

This topic explains some of the general administration that you can perform using Web NMS.

---

- Configuring Log Settings
  - Creating Custom Views
  - Working with Telnet and SSH Session to a Device
-

## 6.12.1 Configuring Log Settings

The Logging Service comes in handy for various purposes, such as pinpointing bugs, configuration errors, performance blockades, creating audit logs, and tracking various actions in the server.

All messages are stored in log files in the form of Text files (.txt). All configurations related to these log files are available in the **logging\_parameter.conf** file located in the <Web NMS Home>/conf directory. The **logging\_parameter.conf** file contains the entries of various user-specified .txt files, the maximum number of lines to be read from a file, and the number of files to be included.

You can configure the logging by editing the **logging\_parameters.conf** file using the **Runtime Administration** tool. Using this tool updates the file at runtime and hence you do not have to restart the Web NMS Server after configuration. But if you have edited the file directly through an editor, ensure to restart the Server.



**Note:** The Runtime Administration Tool can be used to configure the Server-related log messages only. To configure Client-related logs, manually configure the **logging\_paramenters.conf** file located in the <Web NMS Home>/conf directory.

For information on the default log files, refer to Web NMS Log Files in Developer Guide.

- Opening Log File Configuration Tool
- Adding Log Files
- Viewing Log Files
- Modifying Log Files

### Opening Log File Configuration Tool

#### To open the Log File Configuration tool

1. In the Web NMS Client, from **Tools** menu, click **Runtime Administration** or press **Alt+R**. The **Runtime Administration** tool is displayed.
2. From **Categories** drop-down box or tree, choose **Miscellaneous > Log Settings**. The **Logging Configuration** panel is displayed on the right side. The table lists the existing log file names, the directory where it is located in <Web NMS Home>, maximum lines that the file can hold, and the file count.

### Adding Log Files

#### To add a new log file

1. In the Log File Configuration tool, click **Add**. The **Logging Configuration** dialog box is displayed.
2. Specify the name of the log file in the **Log File Name** field.  
**Tips:** Only the file names that are compatible with an OS are supported. | Specify extension as .txt | Avoid numbers.
3. Specify the directory where the log file has to be stored in the **Logging Directory** field. By default, the log files are stored in the <Web NMS Home>/logs directory. If you need to specify a directory within this default location, specify *logs/<directory name>*.

**Example:** If *newlogdir* is specified, a new directory is created in <Web NMS Home> and the new log file is stored in this location. If *logs/newlogdir* is specified, a new directory is created in the <Web NMS Home>/logs directory.

4. Specify the number of lines to be written in the log file in the **Maximum Number of Lines Per File** field. This is an optional field. When no value is specified, the default value of **10000** lines is set.
5. When the log file exceeds the maximum number of lines specified, it is carried forward to another new file that is created with similar name. For example, when newfile.txt reaches 10000 lines, then a new file newfile1.txt is created and the logging continues. The number of files that can be created at such cases can be specified in the **Maximum Number of Files** field.

This is an optional field. When no value is specified, the default value of **10** is set.

6. You can configure the maximum number of lines to be kept in memory before writing them to a log file by specifying the value in the **Maximum Lines Cached** field. For example, if the value is set as 50, the first 50 lines are kept or cached in memory. On reaching the 50th line, all the 50 lines are written to the log file. Then, the second round of writing would happen after caching 50 more lines and so on. This parameter avoids the overhead of frequent writings into the log file for each line.
7. If you require the time stamp along with the log messages, select the **Use Time Stamp?** field.
8. Click **Next**.
9. Specify the unique key name in the **Key Name** field. This serves as the key with which Web NMS differentiates between modules to log module-specific log messages and to identify the type of message, viz., output or error message.
10. Specify the module-specific name that is to be prefixed with the log message in the log file in the **Display Name** field.
11. Click **Add**.
12. Choose the log level from the **Log Level** drop-down box. If you choose to record the messages belonging to certain level, the messages with levels lower than and equal to the level chosen will be recorded. For example, if you choose **Intermediate**, then all the log messages belonging to the **Summary** and **Intermediate** will be recorded.

**Summary:** Important messages

**Intermediate Messages:** Frequently generated log messages

**Verbose:** Detailed/Error messages

**Debug:** Composite of above levels and more information for debugging purposes

13. To enable the logging in this new log file, select the **Enable Logging?** field. If the log file is created with this option not selected, then the log file will be created in the configured directory, but the logging will not take place.
14. Click **Finish**.
15. Click **Apply** to effect changes on the server-side **logging\_parameters.conf** file. The success or failure of writing to server-side file is displayed in the Runtime Administration tool status bar.

## Viewing Details of Log Files

### To view log file details

1. In the Log File Configuration tool, select the log file from the table.
2. Click **View Details**. The **Log Details** dialog box is displayed.

## Modifying Log Files

### To view log file details

1. In the Log File Configuration tool, select the log file to be modified from the table.
2. Click **Modify**. The **Logging Configuration** dialog box is displayed.
3. Make necessary changes in the two screens. For information on each of the fields, refer to Adding Log Files.
4. Click **Finish**.

## 6.12.2 Creating Custom Views

Web NMS client shows a large set of information to the network users. As an Administrator, you may

- **require to show only a subset of information relevant to the user who is monitoring the network's health**

Example: You want a user to monitor only *Critical* events and another user to monitor *Major* events.

- **require to logically group the information shown to the users**

You may want a user to monitor data collection for Routers and Switches. For ease of use, you might want to show the set of Statistics associated to routers and switches separately.

This kind of a segregation in representation of data can be done by creating **Custom Views**. Web NMS modules facilitate creation of custom views to view their objects. For information on creating Custom Views in Map, Fault, and each of the modules, refer to the following links:

- Maps
- Fault
- Audit
- Performance
- Topology

## 6.12.3 Working with Telnet and SSH Session to a Device

AdventNet Web NMS Application/Applet Client supports **Telnet** and **SSH** for managing the devices remotely. Once a device is discovered as a node, Telnet menu is enabled by default.

- Working with Telnet
- Working with SSH

### Working with Telnet

By default, the Telnet option is provided to log in to any remote device discovered in a network.

- Configuring the Telnet to Device menu
- Starting Telnet Session to a device

### Configuring the Telnet Window

Telnet menu available in the maps can be further enhanced by configuring the following additional parameters:

You can implement the following additional features by modifying the **snmpmenu.xml** and **nodeconfig.xml** files located in the <Web NMS Home>/mapdata/menus directory. The configuration files available in <Web NMS Home>/listmenus should also be configured with the same modifications. Ensure to restart the Web NMS Server if you have modified these configuration files.

- Automatic Login
- Setting the Frame Title
- Setting the Font Size
- Setting the Encoding Type
- Setting the Terminal Type
- Setting the Socket Timeout
- Setting the Icon Image
- Closing Telnet Window automatically on disconnecting from Remote Host

#### Automatic Login

To enable automatic login while opening a Telnet Session to a device, configure the following parameters:

**port:** The port in which the Telnet Server is running.

**loginPrompt:** This is the prompt issued by the remote device for getting the user name or login name. Typically this is "login" for Unix systems.

**username:** This is the user name or login name that is present on the system.

**passwordPrompt:** This is the prompt issued by the remote system for getting the password for the user name provided. Typically this is "Password" for Unix systems.

**password:** The password for the user name.

```
<?xml version="1.0"?>
<!DOCTYPE MENU SYSTEM "menu.dtd">
<MENU
.....
.....
```

```
<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe"
action_value="com.adventnet.telnet.telnetwindow.NmsTelnetFrame?host=${ipAddress}&port=23&username=guest&loginPrompt=login:&passwordPrompt=Password:&password=guest"
>
</JAVA-UI>
</MENU-ITEM>
</MENU>
```

**Note:**

1. When the remote device does not prompt for User Name there is no need to set the User Name and Login Prompt.
2. When the remote device does not prompt for Password there is no need to set the Password and Password Prompt.

**Setting the Frame Title**

```
<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe" action_value="com.adventnet.telnet.telnetwindow.NmsTelnetFrame?host=${ipAddress}&frameTitle=MyFrameTitle"
>
</JAVA-UI>
</MENU-ITEM>
```

**Setting the Font Size**

```
<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe"
action_value="com.adventnet.telnet.telnetwindow.NmsTelnetFrame?host=${ipAddress}&fontSize=11"
>
</JAVA-UI>
</MENU-ITEM>
```

**Setting the Encoding Type**

```
<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe" action_value="com.adventnet.telnet.telnetwindow.NmsTelnetFrame?host=${ipAddress}&encoding=gb2312"
>
</JAVA-UI>
</MENU-ITEM>
```

**Setting the Terminal Type**

```
<MENU-ITEM
name="Telnet to device">
<JAVA-UI
```

```

action_type="openframe" action_value="com.adventnet.telnet.te
lnetwindow.NmsTelnetFrame?host=${ipAddress}&terminalType=
vt100">
</JAVA-UI>
</MENU-ITEM>
```

### Setting the Socket Timeout

```

<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe" action_value="com.adventnet.telnet.te
lnetwindow.NmsTelnetFrame?host=${ipAddress}&socketTimeout
=300">
</JAVA-UI>
</MENU-ITEM>
```



**Note:** The Socket Timeout is set in seconds.

### Setting the Icon Image

```

<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe" action_value="com.adventnet.telnet.te
lnetwindow.NmsTelnetFrame?host=${ipAddress}&iconImage=Ima
ge.png">
</JAVA-UI>
</MENU-ITEM>
```



**Note:** The Image (**Image.png**) icon can be placed in **AdventNetCLI.jar** in the **com.adventnet.telnet.telnetwindow** package. It can also be placed in any other directory from where the application starts and the parameter for iconImage has to be set as **/ImagesHome/Image.png**

### Closing Telnet Window automatically on disconnecting from Remote Host

```

<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe"
action_value="com.adventnet.telnet.telnetwindow.NmsTelnetFram
e?host=${ipAddress}&closeOnDisconnect=true">
</JAVA-UI>
</MENU-ITEM>
```



**Note:** If closeOnDisconnect is set to any other value than true / TRUE, the Telnet Window remains open.

### Starting Telnet Session to a Device

On configuring the above parameters, you can start the Telnet Session to a device.

1. In map, select the device for which you need to start a telnet session.
2. Right-click the device and choose **Snmp-Node** or **Node menu > Telnet to Device**. The Telnet window is displayed.



**Note:** The telnet functionality will be invoked using the RMI API "TELNET". Therefore, RMI is necessary for the telnet client to work.

## Working with SSH

SSH is a secured connection between device and Server, which needs valid user name and password to log in. The user has to authenticate before connecting to the device remotely. SSH to Device menu is an optional menu item (not available in Client by default), which can be enabled by configuring Server-side configuration files.



**Note:** SSH is available in two versions, namely SSH1 and SSH2.

- Configuring SSH to Device menu item
- Starting SSH Session to Device

### Configuring SSH to Device Menu Item

#### To enable menu item in Web NMS Client

1. Shut down the AdventNet Web NMS Server and Client before configuring the files.
2. Edit **NmsProcessesBE.conf** file available in <Web NMS Home>/conf directory and modify the process **com.adventnet.nms.telnet.telnetwindow.StartTelnetClient** as given below. If the process is not present in the file, add the following lines:

```
#java com.adventnet.nms.telnet.telnetwindow.StartTelnetClient
[SSH_SUPPORT_REQUIRED true/false]
PROCESS com.adventnet.nms.telnet.telnetwindow.StartTelnetClient
ARGS SSH_SUPPORT_REQUIRED true
```

3. Edit the **NmsProcessesFE.conf** file located in the <Web NMS Home>/conf directory and modify the process **com.adventnet.nms.telnet.telnetwindow.StartTelnetClient** as given below. If the process is not present in the file, add the following :

```
#java
com.adventnet.nms.fe.telnet.telnetwindow.StartTelnetClientFE
[SSH_SUPPORT_REQUIRED true/false]
PROCESS
com.adventnet.nms.fe.telnet.telnetwindow.StartTelnetClientFE
ARGS SSH_SUPPORT_REQUIRED true
```

4. Edit the **nodemenu.xml**, **snmpmenu.xml**, and **routermenu.xml** files located in the <WebNMS Home>/mapdata/menus directory and add the following:

```
<MENU-ITEM name="SSH to device">
<JAVA-UI
action_value="com.adventnet.telnet.telnetwindow.NmsTelnet
Frame?host=${ipAddress}&port=22&sshRequired=true"
action_type="openframe" />
</MENU-ITEM>
```

5. Edit the **nodemenu.xml** and **snmpmenu.xml** files located in the <WebNMS Home>/listmenus directory and add the following:

```
<MENU-ITEM name="SSH to device">
<JAVA-UI
action_value="com.adventnet.telnet.telnetwindow.NmsTelnetFra
me?host=${ipAddress}&port=22&sshRequired=true"
action_type="openframe" />
</MENU-ITEM>
```

## 6. Now start the Web NMS Server.

**Note:**



- For enabling SSH functionality, the parameter **sshRequired** must be set to **true** in the client menu, as shown in the menu item entries given above.
- In case of SSH2, the **JAVA\_HOME** variable of the **setEnv.bat/sh** script must be set to JRE 1.4 or above.

## Starting SSH Session to Device

On configuring the above parameters, you can start the SSH Session to a device.

1. In map, select the device for which you need to start an SSH session.
2. Right-click the device and choose **Snmp-Node** or **Node menu > SSH to Device**. The Authentication dialog box is displayed.
3. Specify user name and password.
4. Click **Login**. The SSH window is displayed.

## Setting the Terminal Type

```
<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe" action_value="com.adventnet.telnet.te
lnetwindow.NmsTelnetFrame?host=${ipAddress}&terminalType=
vt100">
</JAVA-UI>
</MENU-ITEM>
```

## Setting the Socket Timeout

```
<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe" action_value="com.adventnet.telnet.te
lnetwindow.NmsTelnetFrame?host=${ipAddress}&socketTimeout
=300">
</JAVA-UI>
</MENU-ITEM>
```



**Note:** The Socket Timeout is set in seconds.

## Setting the Icon Image

```
<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe" action_value="com.adventnet.telnet.te
lnetwindow.NmsTelnetFrame?host=${ipAddress}&iconImage=Ima
ge.png">
</JAVA-UI>
</MENU-ITEM>
```



**Note:** The Image (**Image.png**) icon can be placed in **AdventNetCLI.jar** in the **com.adventnet.telnet.telnetwindow** package. It can also be placed in any other directory from where the application starts and the parameter for iconImage has to be set as **/ImagesHome/Image.png**

## Closing Telnet Window automatically on disconnecting from Remote Host

```
<MENU-ITEM
name="Telnet to device">
<JAVA-UI
action_type="openframe"
action_value="com.adventnet.telnet.telnetwindow.NmsTelnetFram
e?host=${ipAddress}&closeOnDisconnect=true">
</JAVA-UI>
</MENU-ITEM>
```



**Note:** If closeOnDisconnect is set to any other value than true / TRUE, the Telnet Window remains open.

## Starting Telnet Session to a Device

On configuring the above parameters, you can start the Telnet Session to a device.

1. In map, select the device for which you need to start a telnet session.
2. Right-click the device and choose **Snmp-Node** or **Node** menu > **Telnet to Device**. The Telnet window is displayed.



**Note:** The telnet functionality will be invoked using the RMI API "TELNET". Therefore, RMI is necessary for the telnet client to work.

## Working with SSH

SSH is a secured connection between device and Server, which needs valid user name and password to log in. The user has to authenticate before connecting to the device remotely. SSH to Device menu is an optional menu item (not available in Client by default), which can be enabled by configuring Server-side configuration files.



**Note:** SSH is available in two versions, namely SSH1 and SSH2. For SSH2 support you have to download third-party software.

- Configuring SSH to Device menu item
- Starting SSH Session to Device

## Configuring SSH to Device Menu Item

### To enable menu item in Web NMS Client

1. Shut down the AdventNet Web NMS Server and Client before configuring the files.

2. Edit **NmsProcessesBE.conf** file available in <Web NMS Home>/conf directory and modify the process **com.adventnet.nms.telnet.telnetwindow.StartTelnetClient** as given below. If the process is not present in the file, add the following lines:

```
#java
com.adventnet.nms.telnet.telnetwindow.StartTelnetClient
[SSH_SUPPORT_REQUIRED true/false]
PROCESS com.adventnet.nms.telnet.telnetwindow.StartTelnetClient
ARGS SSH_SUPPORT_REQUIRED true
```

3. Edit the **NmsProcessesFE.conf** file located in the <Web NMS Home>/conf directory and modify the process **com.adventnet.nms.telnet.telnetwindow.StartTelnetClient** as given below. If the process is not present in the file, add the following lines:

```
#java
com.adventnet.nms.fe.telnet.telnetwindow.StartTelnetClientFE
[SSH_SUPPORT_REQUIRED true/false]
PROCESS
com.adventnet.nms.fe.telnet.telnetwindow.StartTelnetClientFE
ARGS SSH_SUPPORT_REQUIRED true
```

4. Perform the additional steps given below for enabling SSH2 support. This requires sshtools (third party package).

- Download the **sshtools-j2ssh-0.0.4-alpha-bin.tar** file from the following URL and extract it.  
<http://prdownloads.sourceforge.net/sshtools>
- Add the jars under <sshtools\_home>/lib to **startnms.sh/bat classpath**. Also set the JAVA home to jre1.4 (or above) in **setenv.bat/sh** available in <Web NMS Home>
- Add a system variable for **sshtools.home** in **startnms.bat/sh**.

```
java ... -Dsshtools.home=<sshtools_home>
com.adventnet.nms.startnms.NmsMainBE
```

5. Edit the **nodemenu.xml**, **snmpmenu.xml**, and **routermenu.xml** files located in the <WebNMS Home>/mapdata/menus directory and add the following:

```
<MENU-ITEM name="SSH to device">
<JAVA-UI
action_value="com.adventnet.telnet.telnetwindow.NmsTelnetFrame?host=${ipAddress}&port=22&sshRequired=true"
action_type="openframe" />
</MENU-ITEM>
```

6. Edit the **nodemenu.xml** and **snmpmenu.xml** files located in the <WebNMS Home>/listmenus directory and add the following:

```
<MENU-ITEM name="SSH to device">
<JAVA-UI
action_value="com.adventnet.telnet.telnetwindow.NmsTelnetFrame?host=${ipAddress}&port=22&sshRequired=true"
action_type="openframe" />
</MENU-ITEM>
```

7. Now start the Web NMS Server.

## Starting SSH Session to Device

On configuring the above parameters, you can start the SSH Session to a device.

1. In map, select the device for which you need to start an SSH session.
2. Right-click the device and choose **Snmp-Node** or **Node** menu > **SSH to Device**. The Authentication dialog box is displayed.
3. Specify user name and password.
4. Click **Login**. The SSH window is displayed.

## 6.13 Advanced Administrative Tasks

This topic explains some of the advanced administrative tasks available in Web NMS.

---

- Front End Server Administration
  - Configuring Transport Mechanism
-

## 6.13.1 Front End Server Administration

Web NMS Front End (FE) Server acts as a link between the Back End (BE) Server and the Clients. The FE can access the database directly when the client request is of type *Read only*, thereby reducing the load on the BE server. However, when the client request involves a *Write* operation, the request goes through the BE server. In the case of BE-FE combination, by default, whenever you start a BE, one FE is also started along with it. Apart from this, you can use the distributed architecture with which you can run standalone FE Server(s) when you need to connect more clients (scalability).

This section explains the common administrative tasks related to the FE server such as

- automatically downloading the configuration files from BE to make the configuration files in BE and FE in synchronization with each other
- configuring the various resources required for running FE
- the configurations required for starting FE when BE is in RMI secure mode

### Downloading Configuration Files at Runtime

In the distributed Web NMS architecture, you can have many FE servers connected to a single BE server. With each FE, you may connect many Clients. All the configuration (conf) files (server-related and client-related) are centrally maintained in BE. The conf files which are FE-related and those related to Clients are separately present in FE(s) and Clients respectively. In the BE server you might be making many configuration changes at runtime. It is always desirable to keep the configuration files of BE in synchronization with those in FE and Clients.

In such a situation, it would be a difficult task to change the configuration files in all the FEs and Clients individually to make them remain in synchronization with the BE's configuration files. To achieve this task with ease, Web NMS provides the *downloading of conf files* mechanism. This mechanism facilitates downloading the conf files from BE to all the FEs and Clients at the time of starting them. This way, you can maintain the configuration files of BE and FE(s) in synchronization with each other.

#### Procedure

In the standalone FE Server installation package, under the <Web NMS FE Home>/conf directory, a file named **DownloadFiles.xml** is available. This file contains the list of configuration files to be downloaded from the BE, when the FE Server is started.

Two distinct tags are present in this file - one for the FE and the other for the Client. The tag for FE is denoted as **<SERVER-FILES>** and the tag for clients is denoted as **<CLIENT-FILES>**.

```

<DOWNLOAD-CONF-FILES>
<SERVER-FILES downloadEachTime="true">
<FILE> conf/serverparameters.conf </FILE>
<FILE> conf/database_params.conf </FILE>
.....
.....
</SERVER-FILES>
<CLIENT-FILES downloadEachTime="true">
<FILE> conf/NmsPanels.conf</FILE>
<FILE> conf/clientparameters.conf</FILE>
.....
.....
<DIR> users/${username}</DIR>
<DIR> html/defaultstoallusers</DIR>

```

```
</CLIENT-FILES>
</DOWNLOAD-CONF-FILES>
```

In the **DownloadFiles.xml** file, there is a tag named **<SERVER-FILES downloadEachTime="">**. If the value for this tag is specified as **true**, all the server-related conf files will be downloaded into FE **each** time when the FE is started. Same is the case with the tag **<CLIENT-FILES downloadEachTime="">**. The **downloadEachTime** parameter in the **<SERVER-FILES>** and **<CLIENT-FILES>** tags is set to **true** by default. It means the configuration files are downloaded each and every time the FE or the Client is connected, i.e., the files get overwritten every time.

When this value is set as **false**, Web NMS checks for the listed files and directories in the FE Server and only the files/directories that are not present in it will be downloaded.

When the value is **true**, the list of files present under the **<SERVER-FILES>** tag will be downloaded when the FE Server is connected to the BE Server. Similarly, the list of files and directories under **<CLIENT-FILES>** tag will be downloaded when the client is connected to the FE Server.

The **<FILE>** tag is used to specify the name of the file that has to be downloaded and the **<DIR>** tag is used to specify the name of the directory to be downloaded (with all its files). The  **\${username}** tag will be replaced at runtime with the user name with which you log into the client. Also, you have the option to add your own files or directories to the list if you want them to get downloaded, along with the default set of files.

### **When to Set downloadEachTime as "false" ?**

This option will be helpful at times when you want to locally modify and maintain the configuration files for the particular FE Server or when you deploy the FE Server in an application server etc.

Any modification in the configuration files in FE will reflect in the Clients connected to the particular FE. These changes will be local to the FE and will not be reflected in the Clients, connected to other FEs.

### **How to use the DownloadFiles.bat/sh in Standalone Mode?**

The **DownloadFiles.bat/sh** file located in the **<Web NMS FEHome>/bin** directory can be used in standalone mode to download the required configuration files without starting the Web NMS servers.

The command line arguments that can be specified in this file are as shown below:

```
com.adventnet.nms.fe.common.DownloadConfFiles BE_HOST localhost
BE_RMI_REG_PORT 1099 ROOT_DIR %NMS_HOME% USER_NAME root
```

Where,

**BE\_HOST:** The host name where the BE Server is running.

**BE\_RMI\_REG\_PORT:** The port number where the RMI registry is listening in the BE Server.

**ROOT\_DIR:** The base/root path to be taken for relative path reference.

**%NMS\_HOME%:** It is taken from the **setEnv.bat/sh** file. The path is set to **<Web NMS FE Home>**.

**USER\_NAME:** The user name whose files and directories have to be downloaded.

The user name parameter is optional. If you want to download the Client configuration files for a particular user, you need to specify that user name in the command line argument in the **DownloadFiles.bat/sh** file.

## Configuring FE Server Resources

For most of its operations, the FE Server depends on the BE Server. Apart from this, the FE requires quite a few other important resources for its functioning. This section provides information about those resources and the procedure for configuring them.

The resources required for FE are

- Database connectivity
- Web Server (Apache)
- Web Container (Tomcat)
- Application Server (EJB mode)

### Database Connectivity

The design of Web NMS is in such a way that the BE and FE servers use the same database. Database-related configuration files are downloaded from BE to the FE during FE startup. Therefore, no separate configuration is required on FE side except adding the driver classes in the classpath in **setEnv.sh/bat**. For more information, refer to the Configuring Database for Web NMS topic.

### Web Server and Web Container (Apache and Tomcat)

Web NMS uses Apache and Tomcat to handle all JSPs, Servlets and HTML pages. The port used by Apache and Tomcat can be changed in the **setEnv.bat/sh** file located in the <Web NMS Home> directory. Changes made here are reflected in all the places where these port numbers are used. By default, WEBSERVER\_PORT and WEBCONTAINER\_PORTS occupy the port numbers 9090 and 8009 respectively. The port numbers are normally specified as shown below:

```
WEBSERVER_PORT=9090
WEBCONTAINER_PORT=8009
```

### Application Server

When Front End Server is deployed in any Application Server such as BEA WebLogic Server 6.0, i.e. for EJB mode, some configurations with respect to the corresponding Application Server can be done.

### Starting FE when BE is in RMI Secure Mode

The Web NMS BE Server can be started in either of the following modes:

- RMI Secure mode
- Normal mode

Starting BE in RMI secure mode, as the name implies, makes the Web NMS RMI APIs secure by making them accessible strictly by the authorized users only. This section explains how the FE can be started when the BE is already running in RMI Secure mode.

### RMI Secure Mode

When the BE is started in secure mode, only a limited number of common module APIs are exposed. But for starting the FE, we require all the common APIs. **RMIAccessAPI** is one among the limited APIs which are exposed to all. The FE can be made to look up the **RMIAccessAPI** to get all the common module APIs, by providing certain information (explained below). The **RMIAccessAPI** takes care of authentication after receiving the required information. It checks whether the user has been authorized to get the common APIs and if so, it allows the user to access them. After getting the APIs, the FE starts.

## Procedure

### Step 1

In the **startnmsFE.bat/sh** file located in the <Web NMSFE HOME>/bin directory, add the following entry:

```
BE_IN_SECURE_MODE true
```

This is to indicate to the FE that the BE is running in RMI Secure mode.

### Step 2

Only the authorized users would be able to access the APIs. To indicate that you are an authorized user, provide the **User Name** and the **Password** in the **startnmsFE.bat/sh** file itself as follows:

```
USERNAME <username>
PASSWORD <password>
```

Supposing, the user name is **root** and the password is **public**, specify as follows:

```
USERNAME root PASSWORD public
```

Alternatively, the user name and the password can be provided in the console. Only if the user name and password are valid, the FE will start.



**Note:** The above user name and password are for starting the FE when BE is running in secure mode only. This is not related to Client authentication i.e., the user name and password which you give for connecting the Client with FE. The Client can be connected to the FE by all the existing users say guest, root, etc.

## Authentication for Accessing BE's APIs

### Utility method PureServerUtilsFE.lookupBEAPI("APINAME")

When BE is in secure mode and also running in a different JVM, authentication would be mandatory for accessing BE's APIs. For accessing any of the BE's APIs, we have provided an utility method named **PureServerUtilsFE.lookupBEAPI("APINAME")**. Just by specifying the name of the API, in the place of "APINAME", you will be able to get the API. This method itself takes care of authentication through the already stored USERNAME and PASSWORD provided at the command line during the startup of FE.

## 6.13.2 Configuring Transport Mechanism

In Web NMS, the communication between the Client and Server takes place through a common connection which uses either TCP Socket or RMI. By default, the communication takes place through TCP. This topic explains how you can change the communication mode to RMI.

This topic explains

---

- Configuring the Mode in BE-FE Combination
  - Configuring the Mode in Standalone FE Server
  - Configuring the RMI Port
- 

### Configuring the Mode in BE-FE Combination

A Web NMS Server is a combination of a BE and an FE Server. Both FE and BE run in the same JVM. You can configure the RMI connection by modifying the **NmsprocessesBE.conf** and **serverparameters.conf** files located in the <Web NMS Home>/conf directory.

In the **NmsprocessesBE.conf** file, the process has to be set to RMI, as shown below:

```
#java com.adventnet.nms.startnms.NmsMainFE [NMS_FE_PORT
WebNMSSocketPort] [USE_QUOTES_IN_DATABASE_TABLES true/false]
[CLIENT_SERVER TCP/RMI/CORBA] [BE_FE TCP/RMI/CORBA] [BE_HOST
back_end_host_name] [BE_PORT back_end_port_num]
[COUNTRY country_code] [LANGUAGE language_code] [ROOT_DIR dir] [
KEEPALIVE_WINDOW_SIZE milliseconds]
PROCESS com.adventnet.nms.startnms.NmsMainFE
ARGS CLIENT_SERVER RMI
```

Configuring the Transport Mechanism using the **serverparameters.conf** file is explained in the next section.

### Configuring the Mode in Standalone FE Server

In standalone FE Server, the configuration has to be done in the **startnmsFE.bat/sh** file located in the <Web NMS FEHome>/bin or in the **serverparameters.conf** file under the <Web NMS Home>/conf directory.

The parameter **CLIENT\_SERVER RMI**, in the **startnmsFE.bat/sh** file, has to be set in the command line argument, as shown below:

```
com.adventnet.nms.startnms.NmsMainFE BE_PORT 2000 BE_HOST localhost
ROOT_DIR %NMS_HOME% CLIENT_SERVER RMI
```

Set the parameter **CLIENT\_SERVER RMI** in the **serverparameters.conf** file, under the <Web NMS Home>/conf directory of the BE Server.

```
#java com.adventnet.nms.startnms.NmsMainFE [NMS_FE_PORT
WebNMSSocketPort]
[CLIENT_SERVER TCP/RMI/CORBA] [BE_FE TCP/RMI/CORBA] [BE_HOST
back_end_host_name] [BE_PORT back_end_port_num] [COUNTRY
country_code] [LANGUAGE language_code] [LOAD_FROM_PRECOMPILED_MIBS
true/false] [ROOT_DIR directory]
CLIENT_SERVER RMI
```

But, if the same parameter is present in the command line argument of the corresponding files, that parameter takes preference, i.e., the configuration in the **serverparameters.conf** file will be overwritten.

## Configuring the RMI Port

To configure the RMI port, changes have to be done in two files, namely **serverparameters.conf** and **transportProvider.conf** located in the <Web NMS Home>/conf directory.

### To configure RMI port

1. Edit the **serverparameters.conf** file.
2. Set the port in the parameter **RMI\_REG\_PORT**. By default, the port number is set as **1099**.  
**Example:** RMI\_REG\_PORT 1100
3. Edit the **transportProvider.conf** file.
4. Set the same port as configured in **serverparameters.conf** in the following argument:

```
CLIENT_CLASS_NAME =
"com.adventnet.management.transport.RMIClientTransportImpl" >
<RMI_REGISTRY_PORT> 1100 </RMI_REGISTRY_PORT>
```

[Top](#)

## 6.14 Administration through Web Client

Besides the Applet, Application and Web Start Clients, most of the administration tasks can also be executed using the Web Client. For more information on Web Client, refer to the Working with Web Client topic in User Guide.

The administrative tasks that you can perform using Web Client are

---

- Admin Configurations: Includes Discovery Parameter Configuration, Discovery Criteria Configuration, Trap Parser Configuration, Logging Configuration.
  - Admin Operations: Includes Shutdown Server, WebNMS Backup, Re-sync with NEs.
  - Server Details: Includes Backend Server Details, Scheduler Details, Port Details, Frontend Server Details, Client Details, Server Logs.
  - Module Details: Includes Discovery Status, Fault Status, Performance Status.
  - User Administration: Includes Add User, Modify User Profile, Remove User, User Details.
  - Network Administration: Includes Add Node, Add Network, Refresh Node.
-

## 6.14.1 Admin Configurations

Administration of Web NMS can be performed at runtime using the Runtime Administration tool. This tool is available in the Application Client, Applet Client, Web Start Client, and Web Client. This tool facilitates configuring the discovery, trap parser, and the log files in Web NMS. This section explains the use of Runtime Administration in Web Client. For information on using the Runtime Administration tool in the other Clients, refer to Runtime Administration topic.

- Discovery Parameter Configuration
- Discovery Criteria Configuration
- Trap Parser Configuration
  - Adding a Trap Parser
  - Loading Trap Parsers
  - Saving the Trap Parser Information to a File
  - Enabling and Disabling Trap Parsers
  - Deleting Trap Parsers
- Logging Configuration



### Discovery Parameter Configuration

Discovery Configuration is about configuring the process of discovery based on entries in the **seed.file** located in the <Web NMS Home>/conf directory. Following configurations can be performed with ease from the Runtime Administration page of Web Client.

- auto discovery of nodes and networks
- discovery of local networks
- enabling log messages
- rediscovery of the already discovered networks or nodes
- setting time interval for discovery
- setting SNMP properties
- setting the ICMP protocol properties

#### To perform Discovery Parameter Configuration

1. In the Web Client, click the **Admin** module tab.
2. Click **Complete View** or the **Admin Configurations** node on the left-side tree of the displayed page.
3. Click **Discovery Parameter Configuration**. The **Discovery Configuration Settings** page is displayed. Each of the fields in this page is tabulated below:

Field	Description
Common Parameters	Options, such as auto discovery, discovering local networks, enabling log message generation, and rediscovering elements can be configured through the displayed page. For information on each of these options, refer to the General Configuration section in the Using Discovery Configurator topic.
SNMP Properties	This section provides options to configure the discovery of SNMP devices. For information on each of these options, refer to the Protocol Configuration section in the Using Discovery Configurator topic.

Field	Description
ICMP Properties	The ICMP ping is performed by Web NMS Discovery engine to detect active devices of a network. You can configure the ping timeout period and the number of times a device is to be pinged at runtime.  <b>Ping Timeout:</b> Specify the duration until when a device is in the pinged state.  <b>Ping Retries:</b> Specify the number of times a device is to be pinged.
Rediscovery Scheduler	To schedule the discovery of devices, click this option. The <b>Rediscovery Scheduler</b> is displayed.  For information on each of these fields, refer to the Scheduling Rediscovery section in the Using Discovery Configurator topic.



## Discovery Criteria Configuration

You can configure the criteria based on which a device or network is to be discovered, at runtime.

### To perform Discovery Criteria Configuration

1. In the Web Client, click the **Admin** module tab.
2. Click **Complete View** or the **Admin Configurations** node on the left-side tree of the displayed page.
3. Click **Discovery Criteria Configuration**. The **Discovery Criteria Configuration** page is displayed.
4. Select the **Allow Criteria** if you want the discovery to happen based on a criteria. Unchecking the box will prevent the device or network from being discovered based on the set criteria.
5. Choose the criteria from the drop-down box and specify the corresponding value in the text field.
6. Click **Add** to add the value specified for the chosen criteria. The added value is listed in a tabular format.
7. Click **Modify** if you want to modify the existing value of a chosen criteria. Click **Delete** to delete the criteria.

For more information, refer to Criteria Based Discovery section in Using Discovery Configurator topic.



## Trap Parser Configuration

The Trap Parsers are used to set criteria for the traps, which in turn generates events. The event properties too can be defined using the Trap Parser. You can add one or more number of Trap Parsers by configuring the **trap.parsers** configuration file located in the <Web NMS Home>/conf directory. The configuration can be performed using the Web Client as explained in this section.

### To access Trap Parser Configuration page

1. In the Web Client, click the **Admin** module tab.
2. Click the **Complete View** or **Admin Configurations** node on the left-side tree of the displayed page.
3. Click **Trap Parser Configuration**. The **Trap Parser Configuration** page is displayed.

## Adding a Trap Parser

### To add a Trap Parser

1. In the **Trap Parser Configuration** page, click **Add Trap parser**. The **Add New Parser** page is displayed.
2. Specify appropriate values in the available fields. For information on each of the fields, refer to Appendix.
3. To add more user properties, click **Add More Properties** and specify the property name and value.
4. Click **Submit**.

## Loading Trap Parsers

### To load Parsers from MIB or File

1. In the **Trap Parser Configuration** page, click **Load Parsers**. The **Load parsers** page is displayed.
2. To load Trap Parser from MIB, choose the MIB from the **MIB File Name** drop-down box and click **Load**. The selected MIB's trap parsers are stored in the **trap.parsers** file located in the <Web NMS Home>/conf directory.
3. To load Trap Parser from file, specify the file name (with the relative path of the folder in Web NMS) in **Filename** field. Click **Load**.

**Note:** The Parsers with the same matching criteria will be overwritten in the **trap.parsers** file.

## Saving the Trap Parser Information to a File

### To save the Parsers to a File

1. In the **Trap Parser Configuration** page, click **Save to File**. All loaded Parsers are displayed.
2. Select the parsers which are to be saved in a file.
3. Specify the name of the file in which the Parsers are to be saved in the **Save Parsers to file** text field. By default, the Trap Parsers are saved in the **trap.parsers** file located in <Web NMS Home>/conf directory.. **Example:** newtrap.parsers
4. Click **Save to file** to save the parsers.

## Enabling and Disabling Trap Parsers

### To enable/disable Trap Parsers

1. The **Trap Parser Configuration** page displays all the loaded Parsers.
2. To enable Trap Parsers, select the parsers which are to be disabled (**Tip:** The Enabled status is displayed with the tick next to the Trap Parser name) and click **Enable**.
3. To disable Trap Parsers, select the disabled parsers which are to be enabled (**Tip:** The Disabled status is displayed with the X symbol next to the Trap Parser name) and click **Disable**.

## Deleting Trap Parsers

### To delete Trap Parsers

1. The **Trap Parser Configuration** page displays all the loaded Parsers.
2. Select the Trap Parsers that you need to delete.
3. Click **Delete**.



## Logging Configuration

The Logging Service comes in handy for various purposes, such as pinpointing bugs, configuration errors, performance blockades, creating audit logs, and tracking various actions in the server.

All messages are stored in log files in the form of Text files (.txt). All configurations related to these log files are available in the logging\_parameter.conf file located in the <Web NMS Home>/conf directory. The logging\_parameter.conf file contains the entries of various user-specified .txt files, the maximum number of lines to be read from a file, and the number of files to be included.

You can configure the logging by editing the **logging\_parameters.conf** file using the Runtime Administration tool. Using this tool updates the file at runtime.

### To configure logging

1. In the Web Client, click the **Admin** module tab.
2. Click the **Complete View** or **Admin Configurations** node on the left-side tree of the displayed page.
3. Click **Logging Configuration**. The **Logging Configuration** page is displayed.
4. The displayed page contains the log **FileName** along with the configurable options, such as **MaxLines**, **FileCount**, **MaxLinesCached**, and **LogLevel**.

Configurable Options	Description
MaxLines	Specify the number of lines to be written in the log file.
FileCount	When the log file exceeds the maximum number of lines specified, it is carried forward to another new file that is created with similar name. For example, when newfile.txt reaches 10000 lines, then a new file newfile1.txt is created and the logging continues.  Specify the maximum number of log files that can be written by Web NMS in this field.
MaxLinesCached	This parameter is used to configure the maximum number of lines to be kept in memory before writing them to a log file.  For example, if the value is set as 50, the first 50 lines are kept or cached in memory. On reaching the 50th line, all the 50 lines are written to the log file. Then, the second round of writing would happen after caching 50 more lines and so on. This parameter avoids the overhead of frequent writings into the log file for each line.
LogLevel	This parameter is used to categorize the log messages into various levels. The four type log levels are <ul style="list-style-type: none"> <li>• <b>Summary:</b> Denotes important messages, such as TftpAPI bound in registry, SeverityAPI bound in registry, NmsPolicyAPI bound in registry, etc.,</li> <li>• <b>Intermediate:</b> Denotes frequently generated log messages, such as Registering Session : AUTH ID,</li> </ul>

Configurable Options	Description
	<p>Registering Session: CONFIG_CLIENT, etc.</p> <ul style="list-style-type: none"> <li>• <b>Verbose:</b> Denotes error messages, such as "Cannot get snmp values from 192.168.4.28 : Error: Request Timed Outto192.168.4.28", etc.</li> <li>• <b>Debug:</b> Denotes DEBUG messages useful for debugging purposes. This level records all the messages belonging to the above three levels and in addition, it records the messages which help in tracing bugs.</li> </ul> <p>The default log level is <b>3</b>.</p>

5. On specifying appropriate values, click **Submit** to update the configured values in the **logging\_parameters.conf** file. Click the **Reset** button, if required, to reset to default values.

#### To configure module-wise logging

Certain log files, such as nmserr.txt and nmsout.txt contain the logging details of various Web NMS modules such as Map, Topology, Provisioning, etc. To configure the logging levels for these modules perform the following procedure.

1. In the **Logging Configuration** page, click **Configure Log Level for <file\_name>** (for nmserr.txt and nmsout.txt files). The **Configure Log Level for <file\_name>** page is displayed.
2. Select the required modules. **Example:** TOPOERR of nmserr.txt file whose log level is to be modified.
3. Choose the **Logging Level** from the drop-down box for the specific module.
4. Click **Submit**. Click **Reset** button, if required, to reset to default values.

## 6.14.2 Admin Operations

- Shutting Down Web NMS Server
- Performing Backup
- Re-sync with NEs



### Shutting Down Web NMS Server

#### To shut down the server

1. Click the **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View** or **Admin Operations** node on the left-side tree of the displayed page.
3. Click **Shutdown Server**.
4. A confirmation is asked. Click **Yes** to shut down the server.



### Performing Backup

#### To backup

1. Click the **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View** or **Admin Operations** node on the left-side tree of the displayed page.
3. Click **WebNMS Backup**.
4. A confirmation is asked. Click **Yes**. A backup of the available data is taken and stored in files under the <Web NMS Home>/conf/backup directory.

### Re-sync with NEs

When there is excessive trap generation from NEs due to some problem, a pileup of trap (that needs to be processed) is created in memory and flat files in Web NMS. This leads to heavy load on the Web NMS and eventually the latest status of the NEs is not displayed in the Client. To get the latest status of all the devices, you can re-synchronize Web NMS with the NEs.

On re-synchronizing,

1. Web NMS stops listening for traps from NEs.
2. All the traps (that are yet to be processed) in the memory and trap files are discarded.
3. Event and Alert tables are deleted from the database and all the NEs are made to *clear* severity.
4. Web NMS starts listening for traps from NEs.
5. Further, a status polling is performed for the NEs and the latest status is updated in the database and depicted in the Client.

There are two ways in which you can re-sync Web NMS with the NEs:

- **Re-sync with NEs after taking Backup:** On re-synchronizing, event and alarm tables are deleted from the database. If you need to backup the data in those tables before re-synchronization, use this option.

- **Re-sync with NEs:** If you don't require to backup event and alarm tables before re-synchronization, use this option.



### Re-sync with NEs after taking Backup

#### To re-sync with NEs after taking backup

1. Click the **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View** or **Admin Operations** node on the left-side tree of the displayed page.
3. Click **Re-sync with NEs after backup**.
4. A confirmation is asked. Click **Yes**.

On performing this, the backed up data is stored in **.data** files and located in <Web NMS Home>/backup directory. **Example of file name:** *BackUp\_APR26\_2004\_15\_24.data*.



### Re-sync with NEs

#### To re-sync with NEs (without taking backup)

1. Click the **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View** or **Admin Operations** node on the left-side tree of the displayed page.
3. Click **Re-sync with NEs**.
4. A confirmation is asked. Click **Yes**.

### 6.14.3 Server Details

Using the Web Client, you can view the details of the Web NMS Server, such as information on back end (BE) and front end (FE) servers, schedulers, ports in use, and the Clients. These details help you in ascertaining the performance of the Web NMS Server and thereby administer it appropriately. For example, to ascertain if there are any threading issues, you can view the details of the schedulers.

- Viewing Back End Server Details
- Viewing Scheduler Details
- Viewing Port Details
- Viewing Front End Server Details
- Viewing Client Details
- Viewing the Server Log Files



#### Back End Server Details

##### To view back end server details

1. Click **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View or Server Details** node on the left-side tree of the displayed page.
3. Click **Backend Server Details**.

Backend Server Details	
Host Name	anna
Host Address	192.168.111.53
Server Started At	Mon May 17 09:48:16 GMT+05:30 2004
OS Name	Windows 2000
Database Name	MYSQL
Total Memory	52 MB
Free Memory	27 MB

The information on the machine where the Web NMS BE server is running is displayed. The information, such as Host Name, Host Address, Server Started At, OS Name, Database Name, Total Memory, and Free Memory is displayed. An example screen shot is given above.



#### Scheduler Details

##### To view Scheduler details

1. Click **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View or Server Details** node on the left-side tree of the displayed page.
3. Click **Scheduler Details**.

The information on the main, SchedulerForFailOver, BEModuleDispatcher, provisioning, policy, statuspoll, config, datapoll, discovery, and UpdateProcessor schedulers is displayed. An example screen shot is given below.

Scheduler Details					
Index	Name	Task Count	Thread Count	Active Threads	Idle Threads
1	main	11	4	0	4
2	SchedulerForFailOver	0	2	0	2
3	BEModuleDispatcher	0	2	1	1
4	policy	0	1	0	1
5	config	1	1	0	1
6	statuspoll	102	3	0	3
7	datapoll	89	3	0	3
8	discovery	1	4	0	4



## Port Details

### To view Port details

1. Click **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View or Server Details** node on the left-side tree of the displayed page.
3. Click **Port Details**.

Information on the ports that are currently occupied by Web NMS is displayed. An example screen shot is given below.

Port Details	
RMI Registry Port	1099
NMS BE Port	2000
WebServer Port	9090
WebContainer Port	8009
Tomcat Shutdown Port	8005
Trap Ports	162



## Front End Server Details

### To view Front End Server details

1. Click **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View or Server Details** node on the left-side tree of the displayed page.
3. Click **Frontend Server Details**.

A list of FE servers that are connected to the BE is displayed. It provides information on the Host Name (where FE server is running), Host Address (IP address of the machine where FE server is

running), Server Mode (Primary or Secondary), Client Communication Mode, RMI Registry Port, and Web Server Port.



## Client Details

### To view Client details

1. Click **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View** or **Server Details** node on the left-side tree of the displayed page.
3. Click **Client Details**.

Information on the Clients that are connected to the BE is displayed.

<b>Front End Server</b>	The FE server host name that is connected to the BE.
<b>Client Type</b>	The type of client connected to the BE. It includes Application, Applet, and Web Start Clients.
<b>User Name</b>	The Client's login name (user) using which the client is being accessed.
<b>Client started at</b>	The time at which the client was started/connected to the BE. <b>Example:</b> <i>Wed Apr 07 16:55:04 GMT+05:30 2004</i>



## Viewing the Server Log Files

### To view the server logs

1. Click the **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View** or **Server Details** node on the left-side tree of the displayed page.
3. Click **Server Logs**. All server log files are listed.
4. Click a log file to view its details. The log file is displayed in a new window.

## 6.14.4 Module Details

- Viewing Discovery Status
- Viewing Fault Status
- Viewing Performance Status

Using the Web Client, you can view the details of Web NMS modules, such as Discovery, Fault, and Performance. This helps you in ascertaining the functioning of a module.



### Viewing Discovery Status

#### To view discovery status

1. Click **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View or Module Details** node on the left-side tree of the displayed page.
3. Click **Discovery Status**. The following tabulated information is displayed.

<b>Discovery Module Details</b>	
Network Count	Total number of networks discovered.
ManagedObject Count	Total number of Managed Objects (MO) created.
Node Count	Total number of nodes discovered in the network.
Interface Count	Total number of interfaces discovered in the network elements.
<b>Network Discovery Status</b>	
IP Address	IP address of the discovered network.
Discovery finished at	The time at which the discovery of this network was completed. <b>Example:</b> Wed Apr 07 15:36:10 GMT+05:30 2004
Rediscovery scheduled at	The time at which the next rediscovery process is scheduled. <b>Example:</b> Thu Apr 08 15:36:10 GMT+05:30 2004



### Viewing Fault Status

#### To view fault status

1. Click **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View or Module Details** node on the left-side tree of the displayed page.
3. Click **Fault Status**.

Information on the Events and Alerts in the queue that are to be sent, traps that are yet to be processed, and the time at which the last trap was received, is displayed.



### Viewing Performance Status

#### To view performance status

1. Click **Admin** module tab. The Admin page is displayed.
2. Click the **Complete View or Module Details** node on the left-side tree of the displayed page.

3. Click **Performance Status**.
4. Specify the node name for which you need to view performance statistics in **Node Name** field.
5. Click **View Status**.

<b>Name</b>	OIDs for which statistics is being collected.
<b>Avg. polls per hour</b>	Number of times polling has been performed for the configured time.
<b>Success poll cycles</b>	The success rate of the polling for the configured time.
<b>Poll interval in seconds</b>	The interval at which the status polling is performed. It is displayed in seconds.
<b>Data Collection Enabled</b>	Specifies whether data collection is enabled for that device.  <b>true</b> - Enabled <b>false</b> - Disabled
<b>Last collection time</b>	The time when data collection was last performed.
<b>Next collection time</b>	The time when data collection is to be performed next.

From this page, if you need to view performance statistics for any other node,

1. Specify the node name in **Node Name** field.
2. From **Period** drop-down box, choose the period for which you need to view performance statistics. It includes **Today**, **Last 7 Days**, **Last 30 Days**, and **Custom**.  
  
If **Custom** is selected in **Period** drop-down box, specify the **Start Date** and **End Date**, the range between which you need to view the performance statistics.
3. Click **View Status**.

## 6.14.5 Web Client: User Administration

- 
- Adding a New User
  - Modifying a User's Profile
  - Removing a User
  - Viewing User Details
- 



### Adding a New User

#### To add a new user

1. Click **Admin** module tab. The Admin page is displayed.
2. Click **User Admin** from the **Admin** tree displayed on the left side frame.
3. Click **Add new user** from the left side tree or click **Add User** from the **User Admin** page displayed on right side frame. The **Add User** form is displayed.
4. Enter the new name for the user in **User name** field.
5. Enter a password in the **Password** field and re-enter the same password in **Re-type Password** field.
6. The **Available group names** field lists all the existing groups. Select the group(s) to which the user should be a member.  
If you need to add the user to a new group, select the **Add this user to a new group** check box and enter the name of the new group in the text field.
7. Select the **Password expires in** check box and enter the number of days the password stays valid. If this check box is not selected, then the password never expires.
8. Similarly, select the **Account expires in** check box and enter the number of days the user account stays valid. If this check box is not selected, then the user account never expires.
9. Click **Add User**.

On performing this, a confirmation message on the success or failure of the configuration is displayed.



### Modifying a User's Profile

#### To modify a user's profile

1. Click **Admin** module tab. The Admin page is displayed.
2. Click **User Admin** from the **Admin** tree displayed on the left side frame.
3. Click **Modify User Profile** from the left side tree or from the **User Admin** page displayed on right side frame. The **Modify User Profile** form is displayed.
4. Enter an existing user's name whose profile you need to edit in the **User Name** field.
5. Click **Submit**. The **Modify profile** page is displayed.
6. Select **Change Password** check box if you need to change that user's password.  
Enter the existing password in **Current Password** field. Enter the new password and re-enter the same password in **New password** and **Re-type password** fields respectively.

7. Under **Group options**, the **Enrolled groups** field lists the group(s) in which the user has already been enrolled. The **Available groups** field lists the existing groups that the user has not been enrolled. Use the **Remove**  and **Add**  options to remove the user from a group or enroll the user to a group.
8. The **Modify password expiration** field displays the number of days the password stays valid. If this was not configured while creating the user, then **0** is displayed, which means the password never expires. Modify the expiration period, if required, by selecting the check box and entering a new value in the text field.
9. The **Modify account expiration** field displays the number of days the user account stays valid. If this was not configured while creating the user, then **0** is displayed, which means the user account never expires. Modify the expiration period, if required, by selecting the check box and entering a new value in the text field.
10. On editing the required fields, click **Submit**.

On performing this, a confirmation message on the success or failure of the configuration is displayed.



## Removing a User

### To remove a user

1. Click **Admin** module tab. The Admin page is displayed.
2. Click **User Admin** from the **Admin** tree displayed on the left side frame.
3. Click **Remove User** from the left side tree or from the **User Admin** page displayed on right side frame. The **Remove User** form is displayed.
4. Enter an existing user's name in **User name** field.
5. Click **Submit**.

On performing this, a confirmation message on the success or failure of the configuration is displayed.



## Viewing User Details

### To view the user details

1. Click the **Admin** module tab. The Admin page is displayed.
2. Click the **System Admin** link located on the left side. The **System Admin** page is displayed.
3. To view details of the available groups and the users in those groups, click **Group Based List**.
4. To view details of the available users and the groups to which they are associated, click **User Based List**.
5. To view the list of users logged into the current session, click **Active Users List**.

## 6.14.6 Web Client: Network Administration

- 
- Adding a New Network
  - Adding a New Node
  - Refreshing a Node
- 



### Adding a New Network

Networks and their elements are discovered automatically by Web NMS and the discovery process is carried out in a predetermined way. If you need to discover a network or node manually instead of waiting for Web NMS to discover it automatically, use the **Add New Network** and **Add New Node** options.

#### To add a new network

1. Click **Admin** module tab. The Admin page is displayed.
2. Click **Network Admin** from the **Admin** tree displayed on the left side frame.
3. Click **Add Network** from the left side tree or from the **Network Admin** page displayed on right side frame. The **Add New Network** page is displayed.
4. Enter a valid IP Address in **Network Address** field and select the netmask (by default 255.255.255.0) from **Netmask** combo box.
5. The **Discovery Configuration** options provided are optional. The significance of each of the fields is given below.

Field	Significance
<b>Start Discovery</b>	If this option is selected, the discovery of the network added starts instantly.  If the option is not selected, then the network is just added to the database but discovery of that network is not performed.
<b>Manage the Network</b>	If this option is selected, the network is added to the database and discovery happens. The network and its elements are in managed state as they are discovered.  If this option is not selected, the network is added in unmanaged state to the database and discovery of that network will not be started. Hence none of the network elements in the network will be discovered.
<b>Override the discovery configuration</b>	Initially some configurations are made related to discovery in the seed.file using Discovery Configurator tool. A configuration could have been made to restrict the discovery of certain IPs. But if you select this option, those configurations are overridden and discovery is performed.
<b>Update the discovery configuration</b>	If you want this network to be discovered the next time Web NMS Server is started (after reinitializing), select this option. On doing so, the IP that you mention is configured in the seed.file (discovery configuration file present in <Web NMS Home/conf directory>) permanently.

6. Once the **Add Network** operation is committed, Web NMS takes a while to discover the network and its elements. If you do not want to wait for the discovery to be completed and want to proceed with other operations, select **Process in the background check ox**. By doing so, you can quit the current view and work on other views while the discovery process is done in the background.

7. Click **Add**.

If the network IP that you have entered has already been added to the database and discovered by Web NMS, relevant message is displayed in the **Add New Network** page.

Use the Details Sheet to view information on the newly added network.



## Adding a New Node

### To add a new node

1. Click **Admin** module tab. The Admin page is displayed.
2. Click **Network Admin** from the **Admin** tree displayed on the left side frame.
3. Click Add Node from the left side tree or from the Network Admin page displayed on right side frame. The Add New Node page is displayed.
4. Enter a valid IP Address in **IP Address** field and select the netmask (by default, 255.255.255.0) from **Netmask** combo box.
5. The significance of each of the fields under **SNMP Configuration** and **Discovery Configuration** is given below.

Field	Significance
<b>SNMP Configuration</b>	
<b>SNMP Port</b>	Port number where the SNMP agent is running. By default, the port is 161.
<b>Community</b>	By default, the value is public. When no value is set, then the community value as configured in the seed.file is fetched and substituted.
<b>Enable V3 (User Name, Context Name)</b>	If you enable the discovery of SNMPv3 devices, then you need to specify the user name and context name in the corresponding field.
<b>Discovery Configuration</b>	
<b>Discover even if the node is not reachable</b>	If this option is checked, even if the node is not alive when you add it, Web NMS adds a managed element for that node.
<b>Discover all the devices in the parent network</b>	If this option is selected, apart from adding the node that you have configured, all other devices in their parent network are also discovered (if they were not discovered already).  For example, if you add a device 192.168.1.5 with this option checked, then all the devices in the 192.168.1.0 network are also discovered.
<b>Override discovery configuration</b>	Initially some configurations are made related to discovery in the seed.file using Discovery Configurator tool. A configuration could have been made to restrict the discovery of certain nodes. But if you select this option, those configurations are overridden and discovery is performed for those nodes also.

Field	Significance
<b>Update discovery configuration</b>	If you want this node to be discovered the next time the Web NMS Server is started (after reinitializing), select this option. On doing so, the node that you mention is configured in the seed.file (discovery configuration file present in <Web NMS Home>/conf directory) permanently.

6. Once the **Add Node** operation is committed, Web NMS takes a while to discover the node. If you do not want to wait for the discovery to be completed and want to proceed with other operations, select **Process in the background** check box. By doing so, you can quit the current view and work on other views while the discovery process is done in the background.
7. Click **Add Node**.

If the node IP that you have entered has already been added to the database and discovered by Web NMS, relevant message is displayed in the **Add Node** page.

Use the Details Sheet to view information on the newly added device.



## Refreshing a Node

To rediscover a node in the network, use the **Refresh Node** option. A node or device could have been down for a while or it would not have been discovered when you performed a manual discovery of that node. In these cases, refresh the node manually to obtain its latest information.

### To refresh a node

1. Click **Admin** module tab. The Admin page is displayed.
2. Click **Network Admin** from the **Admin** tree displayed on the left side frame.
3. Click **Refresh Node** from the left side tree or from the **Network Admin** page displayed on right side frame. The **Refresh Node** page is displayed.
4. Enter the name or IP address of the node to be refreshed in the **Name of the Node** field.
5. Select the netmask (by default, 255.255.255.0) from **Netmask** combo box.
6. Enter the port (by default, 161) where SNMP agent is running in **SNMP Port** field.
7. Click **Refresh**.

A node can be refreshed also from the Network Map and Network Database views.

## 6.15 Simulators and Browsers

This topic explains the various simulators and browsers that are bundled with Web NMS. Some of the links in this page takes you to the Studio help documentation.

- **MIB Browser**

The MIB Browser enables loading of MIBs, searching MIBs, walking the MIB tree, and performing all other SNMP related functions. MIB Browser helps you to view and operate the data available in a managed device through an SNMP agent.

- **TL1 Craft Interface**

The TL1 Craft Interface is a full fledged GUI application that can be used to query a TL1 device and get responses. It allows the user to view and operate on data available through a TL1 agent on a managed device thereby managing the device.

- **CLI Browser**

The CLI Browser is a GUI experienced network management application that supports Command Line Interface and can be used to manage network devices. You can use CLI Browser to communicate with network devices such as routers, switches, remote machines, and others.

- **Multi Protocol Browser**

The Multi Protocol Browser is a debugging tool and is used to verify management operations for Device Information Bases such as MIB, TL1 Command Set, MO Classes, and XML generated by screens to communicate with Management Server.

- **SNMP Agent Simulator**

The SNMP Agent Simulator is used to simulate an SNMP agent through configuration or by recording data from an existing SNMP agent. You can simulate SNMP devices such as router, switch, and printer by loading the appropriate MIBs.

- **TL1 Agent Simulator**

The TL1 Agent Simulator is used to simulate a TL1 agent through configuration or by loading the appropriate TL1 Command Set files. TL1 Agent Simulator takes the command set file in the XML format as the input and the UI is designed in a way easy to configure the simulated environment.

- **Non UI Agent**

Non-UI Agent allows you to control the starting and stopping of an agent using the agent configuration file saved in SNMP or TL1 agent simulator. The major advantage of Non-UI agent is that the Multiple agent's can be started at different ports.

- **TL1 Message Builder**

The TL1 Message Builder is used to create and modify TL1 Command Set and Data Set definitions in the XML format. The TL1 Data Set definition file will have possible values for each command defined in TCS.

## 6.15.1 MIB Browser

The MIB Browser is a complete SNMP MIB Browser that enables loading, browsing, and searching MIBs, walking the MIB tree, and performing all other SNMP-related functions. MIB Browser also enables viewing and operating the data available through an SNMP agent in a managed device.

This topic explains:

---

- Starting Up
  - Configuration
  - MIB Operations
  - SNMP Operations
  - Trap Handling
  - Table Handling
  - Graphs
  - Internationalization
  - Debugging and Decoding
  - Error Messages
  - Customization
  - FAQs
-

## 6.15.1.1 Starting Up

---

- Features of MIB Browser
  - Invoking MIB Browser
  - Understanding MIB Browser Work Area
- 

MibBrowser can be invoked as a standalone application or as an applet. The differences in using the MibBrowser as an application and as an applet are highlighted in relevant areas throughout this section.

### Features of MIB Browser

- Enables saving of MibBrowser settings.
- Provides the capability to load and view MIB modules in a MIB tree.
- Helps in traversing the MIB tree to view the definitions of each node for a particular object defined in the MIB.
- Enables to perform the basic SNMP operations, such as GET, GETNEXT, GETBULK, and SET.
- Supports multi-varbind requests.
- Enables real-time plotting of SNMP data in a graph. Line graph and bar graph are the two types of graphs that are currently supported.
- Provides a user-friendly view of SNMP table data. The table data can be viewed in a separate window called SNMP Table Panel.
- Enables to view the incoming traps using Trap Viewer. It also allows parsing of traps.
- Supports internationalization. This feature deploys the applications and applets developed using the AdventNet SNMP API in various languages without altering the code.
- Enables loading of MIBs at startup.

### Invoking MIB Browser

MIB Browser can be invoked as an application or an applet.

#### To invoke MIB Browser

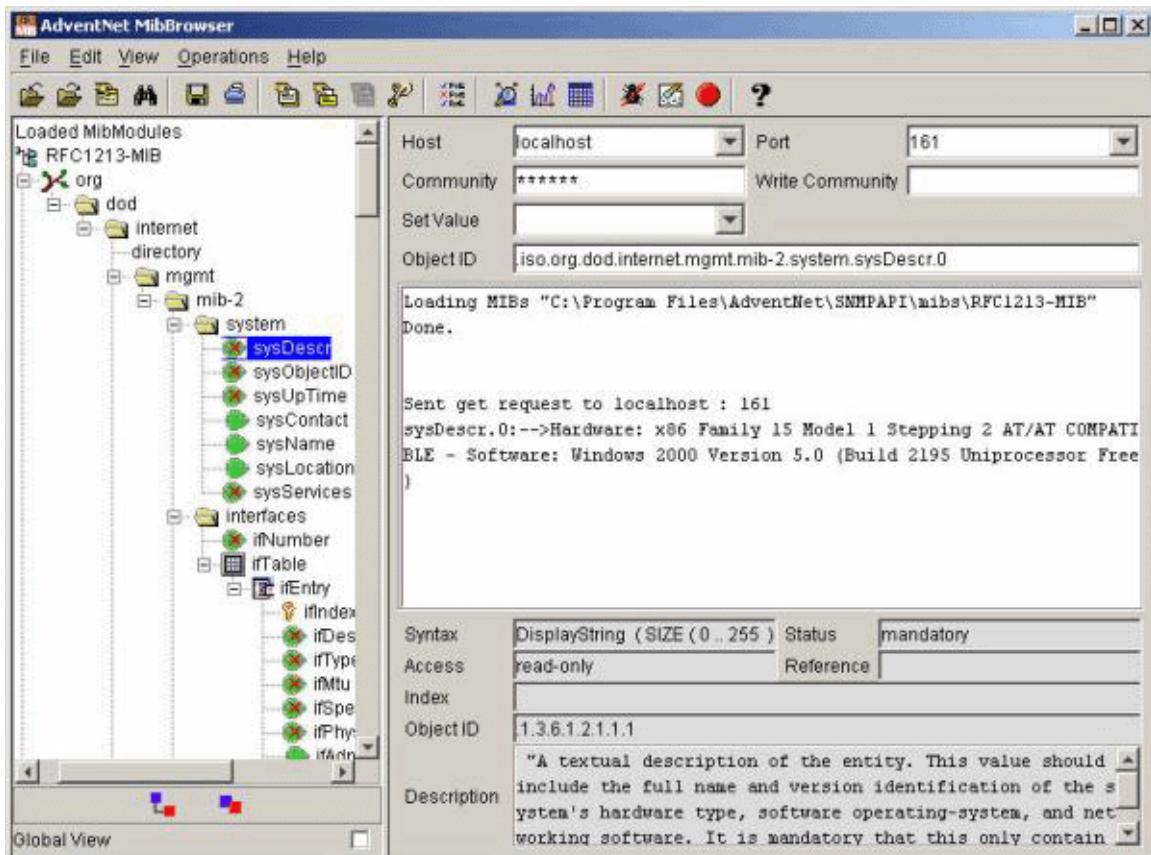
1. Run **MibBrowser.sh/.bat** located in the <Web NMS Home>/bin/browsers directory. Ensure that JAVA\_HOME path is set properly before invoking MIB Browser. You can do this by editing the script/batch file.
2. MIB Browser, by default, can be viewed in both **Java UI** and **Web Client** of the Client Application. However, the Web Client does not support the following features: Menu options, Graphs, Debugging and Decoding, and SNMPv3 related features.
3. The MIB Browser can also be invoked from **Web NMS Launcher > Administrator Tools**.



While invoking MibBrowser from Launcher, the security provider jars should be placed before **AdventNetSntp.jar** in the CLASSPATH for v3 security level. To do this, appropriate changes need to be done in the MibBrowser section of the **launcher\_conf.txt** file.

This section gives an overview of AdventNet MibBrowser and highlights its features. It also gives an illustrative overview of the user interface and an extensive focus on the various SNMP operations that can be done using MibBrowser.

## Understanding MIB Browser Work Area



The image above depicts the primary window of AdventNet MibBrowser. It consists of a

- **menu bar:** Displays a list of commands to perform various operations.
- **toolbar:** Displays buttons with images that act as shortcuts to the menu options.
- **left frame:** Holds the MIB tree. A MIB tree is a structure that displays all the loaded MIBs. The MIB tree enables to traverse the tree, view the loaded MIBs, and the definition of each node.
- **right frame:** Contains text fields to specify the basic parameters, such as host, community, and so on. It also contains a text area to display the results.

There are three ways in which the primary window of the MibBrowser can be displayed. They are the **Result Display**, **MIB Description**, and **Multi-Varbind**. To change the display, click **View > Display** and select the desired view. By default, the MIB Description display is visible in the MibBrowser.

## 6.15.1.2 Configuration

- Setting Common Parameters
- Setting MIB Parameters

AdventNet MibBrowser can be used to view and operate on the data available through an SNMP agent. MibBrowser can be configured in tune with performing the SNMP operations.

To configure the MibBrowser, click the **MibBrowser Settings** button  or select **Edit > Settings** from the menu. You can also use the shortcut key combination **Alt + S**.

The MibBrowser Settings dialog box is displayed. It has the following two tabs:

- General
- Mib Settings

### Setting Common Parameters

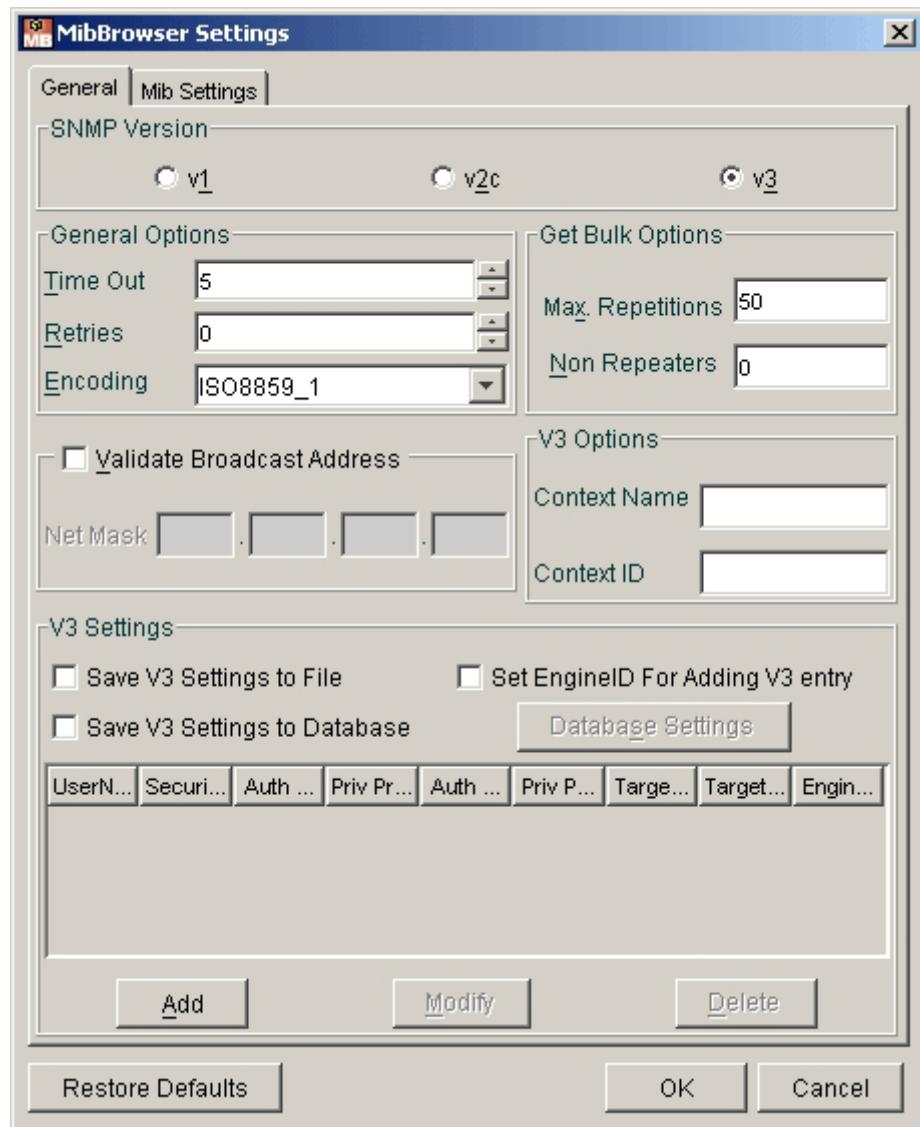
The parameters, such as host, port, and community, can be set in the MibBrowser's main window. Applications use the host name or the IP address of the device to communicate with the agent of the device in a particular port number. This remote port number is the UDP port 161. By default, all the SNMP request messages are received in this port.

SNMP mandates that the SNMP agents should accept request messages only if the community string in the message matches its community name. Therefore, the management application should always communicate with the agents along with the associated community name. The default SNMP community names are "public" for read-only (GET) operations and "private" for read-write (SET) operations. The management applications should have provision to include the community names in their request messages.

Community strings are used to authenticate SNMP PDUs. Since SNMP packets are usually sent using UDP packets, there is no connection established as in the case of TCP/IP packets. Therefore, when a UDP packet is sent to the agent, the agent validates the packet. It accepts and sends a response if the community string of the PDU is equal to that set on the agent, or else drops the packet. The agent does not change the community name after communicating. Applications typically communicate with the SNMP agents by specifying the community name of the agent.

The default community string is "public" and the default Write Community string is null. When Write Community is null, community itself is used for SET operations. Therefore, applications should explicitly set the Write Community, before they can use it for SET operations.

The other parameters are set in the General tab of the MibBrowser Settings frame. The general settings include the basic protocol options related to SNMP, the display options, and a section for encoding field. The image depicted below shows the General tab of the MibBrowser Settings dialog box.



The various protocol-related options to SNMP are listed in the table below.

Options	Default Values	Other Options
SNMP Version	v1	v2c or v3
Timeout	5 sec	any user-defined value
Retries	0	any user-defined value
Encoding	ISO8859_1	any encoding scheme that supports text format
Max Repetitions	50	any user-defined value
Non Repeaters	0	any user-defined value

	<ul style="list-style-type: none"> <li>• Timeout is the time interval that an application waits for a response message from an agent before timing out. Retries is the number of times a request is sent when a timeout occurs. If the retry value is 0, the request is re-transmitted on timeout.</li> <li>• The Max-repetitions and Non-repeaters options are enabled only when the SNMP version is set to either v2c or v3. This is because, the GETBULK operation is available only in v2c and v3. A GETBULK request is performed by giving an OID along with two other parameters, Max Repetitions value and Non Repeaters value.</li> <li>• Encoding, in general, means, modifying information into the required transmission format. Computers around the world store information using a variety of encoding schemes. AdventNet MibBrowser support the ISO8859_1, which means ISO 8859_1, Latin alphabet No.1. There are various other encoding schemes that support various text formats. You can use the encoding scheme that best suits your requirement while performing SNMP operations. To view the encoding scheme that is supported by Java Development Kit, see:  <a href="http://java.sun.com/products/jdk/1.1/docs/guide/intl/encoding.doc.html">http://java.sun.com/products/jdk/1.1/docs/guide/intl/encoding.doc.html</a>.</li> </ul>
---	--

The Validate Broadcast Address check box enables you to check the validity of the broadcast address provided. You need to provide the Netmask address to validate the broadcast address. A Netmask is a string of 0's and 1's that hides the network part of the IP address and allows only the host ID to remain.

In the v3 Options section, Context Name and the ContextID are to be provided as additional parameters for an SNMPv3 request. An SNMP context name 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, any management application can access that information by giving that context name. The ContextID uniquely identifies an SNMP entity that may recognize an instance of a context with a particular context name within an administrative domain.

The next section is the v3Settings section. The following are the security-related parameters for accessing the SNMPv3 agents. You can add, modify, and delete users by clicking the Add, Modify, Delete buttons.

Options	Default Values	Other Options
User name	null	any user-defined value
Security level	noAuth noPriv	Auth noPriv and Auth Priv
Authentication Protocol	MD5 (if authentication is chosen in security level)	SHA
Privacy Protocol	CBC-DES (if privacy is chosen in security level)	not available
Authentication password	any user defined value	-
Privacy password	any user defined value	-
Target host	localhost	any host with SNMPV3 agent or proxy agent
Target port	161	any user-defined port

If the security level is "NoAuthNoPriv", no additional parameters are required. If the security level is "AuthNoPriv", the parameters AuthProtocol and AuthPassword are set. If the user security level is "AuthPriv", the privacy password needs to be set in addition to the other parameters.

The v3Settings section has an option for storing the v3 table entries. The v3 table entries can be stored in:

- A serialized file
- A database

### **Storing Table Entries in a Serialized File**

To enable serialization of v3 table entries, select the Save v3 Settings to File option. If this option is selected, the user information is stored in the serialized files namely UserEntry.ser and EngineEntry.ser. When MibBrowser is invoked the next time, the serialized files are deserialized and the v3 table is updated. The advantage of storing table entries in serialized files is that the operation is faster.

### **Storing Table Entries in a Database**

To store v3 table entries in a database, select the Save v3 Settings to Database option. To use this, the database connection has to be established. Clicking the "Database Settings" button displays the Database Parameters dialog box. The image of the dialog box that appears is given below.

Enter the necessary database parameters in this dialog box, and click the OK button. If the database connection is established successfully, all the user information entered is saved in the database. When the MibBrowser is invoked the next time, v3 details are restored and the v3 table is updated.

The advantages of storing v3 table entries in a database are:

- Scalability - Any number of entries can be maintained in the database.
- Accessibility - All the authenticated users of the database can access the entries.

The last section is the field entry section in which the corresponding fields in the v3 table are displayed for data entry. The various buttons available in the field entry section are Add, Modify, and Delete.

To add an entry, enter the required parameters in the respective fields and click the Add Entry button. Based on the parameters and the security level, Discovery and Time Synchronization are done and USM Table is updated and listed in the v3 table.

To modify an entry, select the entry in the v3 table, modify the required fields, and click the Modify button. Time Synchronization is done and the USM table is updated and listed in the v3 table.



The NoAuthNoPriv entry cannot be modified. Only the password fields in the AuthNoPriv entry and AuthPriv entry can be modified.

To delete an entry in the v3 table, select the entry in the v3 table and click the Delete button. The entry is removed from the USM table.



- The settings are saved only on exiting the MibBrowser application and not every time the settings are modified.
- The 'Save v3 Settings to File' option is enabled only in the MibBrowser application and not in the MibBrowser applet because of certain security restrictions in applets.
- The Restore Defaults button is used to reset the default parameters.

## Setting MIB Parameters

The Mib Settings tab is used to load MIBs in MibBrowser. The first section gives the MIB loading options. Refer to Loading MIBs and Unloading MIBs for more details. The next section displays the various parsing levels. Refer to Parsing MIBs for more information.

### 6.15.1.3 MIB Operations

---

- Loading MIBs
  - Unloading MIBs
  - Parsing MIBs
- 

The basic MIB operations are loading, unloading, and parsing MIB files. A MIB file can be loaded directly, or from compiled files, or from a database.

## 6.151.3.1 Loading MIBs

- MIB Loading Options
- Instructions for Using MySQL Database for Loading MIBs
- Instructions for Using Oracle Database for Loading MIBs

Follow the steps given below to load a MIB file.

1. Click the Load MIB Module button  or select **File-->Load MIB** from the menu. Alternatively, you can use the shortcut combination Ctrl + O. This displays the Load a Mib File dialog box.
  2. In the Load a Mib File dialog box, select the MIB file from the mibs folder.
-  If MibBrowser is used as an applet, the URL should be relative to the Web server path. If MibBrowser is used as an application, the specified URL can be absolute or relative. When you use the MibBrowser applet, it is not possible to read a file on some host that is not the applet's host because of the browser security. In the MibBrowser applet, remote browsing of MIB file is supported through SAS.
3. There are other options for loading the MIB file. Click the Recent tab to load the recently loaded MIB files.
  4. Select the check box next to the MIB that is to be loaded and click Open to load the MIB file.



The Load All MIBs option in the File menu loads all the recently loaded MIBs.

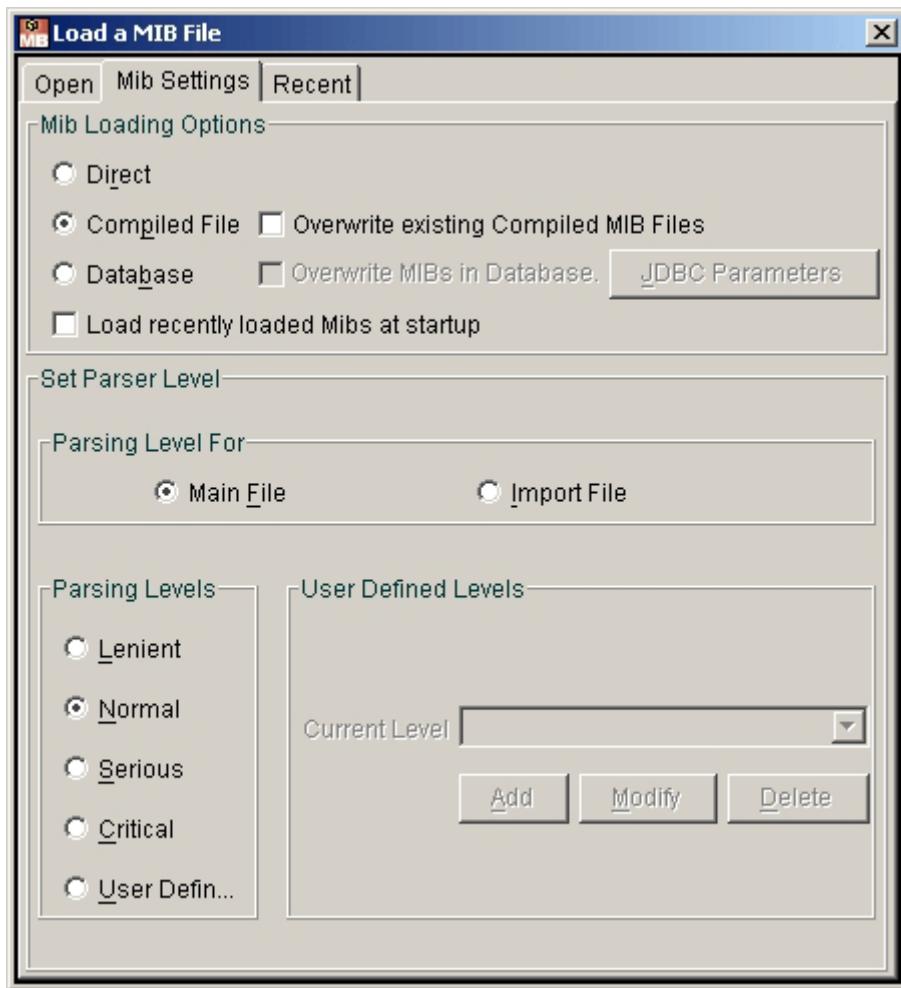
Let us have an overview on the various options available in the MIB Settings section of the Load a MIB File dialog box.

### MIB Loading Options

The various options available for loading MIBs are:

- Load MIBs directly
- Load MIBs from compiled files
- Load MIBs from a database

The following image depicts the Mib Settings tab in the Load MIB dialog box.



### Load MIBs Directly

The MIB file is usually read and parsed into MIB modules and displayed in the MIB tree. In this case, when you load a MIB file, it is parsed and then loaded. This is time consuming because parsing is done every time a MIB file is loaded.

### Load MIBs from Compiled Files

The next option is loading of the MIB files as compiled files. The main advantage here is that the loading time is reduced. This ultimately leads to the improvement in performance. To store the MIB information in a formatted structure, the following two new file types are made available.

- cmi - This file type contains MIB information, such as MibNode, MibModule, naming hierarchy, etc.
- cds - This file type contains the description and reference of the MIB nodes.

When the option Load MIBs from Compiled File is selected, the MibBrowser loads the MIB from the cmi and cds files. If these files are not present, MibBrowser parses the MIB file, writes the output in the cmi and cds files, and loads the MIB file. For example, if you load the RFC1213-MIB, the MIB file is parsed and stored in the compiled MIB files as RFC1213-MIB.cmi and RFC1213-MIB.cds provided RFC1213-MIB is the module name of the RFC1213-MIB file.

When this MIB file is loaded again, the MIB is loaded from the cmi and cds files and no parsing is done. The advantage of using this option is, we need not parse the MIB each time we load, thus optimizing the load time and improving the performance. While loading the compiled MIBs, you need to load only the cmi file. The cmi file has a reference to the cds files. Therefore, the cds file need not be loaded directly.



- Any changes made to the MIB file after it has been loaded as a compiled MIB file are not reflected when it is loaded again. You have to remove the existing cmi and cds files and load the MIB again to view the latest changes. To overcome this, select the option "Overwrite existing Compiled MIB Files". If this option is set to true, the cmi and cds files are created each time the MIB is loaded. However, enabling this option is recommended only if you have changed the contents of the MIB file. Otherwise, this serves as a redundant option and increases the load time of the MIBs.
- In applets, the option of loading MIBs from compiled files has restricted usage. This is because of certain restrictions in file creation. That is, the cmi and cds files cannot be created while loading the MIB file. However, we can load the previously created compiled files by selecting the Load MIBs from compiled File option. Therefore, when no cmi and cds files exist for loading the MIB file, you can select the "Load MIBs directly" option.

To convert the normal MIB files to the cmi and cds format, the `MibToCMI` utility can be used. This class is available in the `<classes/com/adventnet/snmp/utils>` directory. To use the utility, set the `CLASSPATH` to the classes directory and give the following command.

```
java com.adventnet.snmp.utils.MibToCMI directory name or
file, another directory or file
```

The conversion can be done for individual files or for an entire directory of MIB files. If the utility is used across directories, the existing cmi and cds files should first be deleted from the directory.



If the MIB is loaded with the compiled MIBs option with parsing level equal to or above NORMAL and if the MIB has errors, the cmi files will not be created.

## Loading MIBs from a Database

The third option is loading of the MIB files from a database. The MIB files can be stored in any RDBMS such as MySQL or Oracle. Applications can load these MIB files directly from the database. This feature is particularly useful when the MIB files to be loaded are more in number.

The `MibBrowser` uses JDBC (Java Database Connectivity) for the database support. Applications should use a valid JDBC driver of the respective databases to enable the database support.

Selecting the option Load MIBs from Database enables the text fields in the `JDBCParams` section. On initializing the necessary database parameters in this section, the database support can be provided for loading MIBs. The required `JDBCParams` are

- Drivername - name of the database driver.
- URL - URL pointing to the database filename.
- UserName - name of the user.
- Password - password for the user.

After selecting this loading option, select the required MIB file to be loaded from the Open tab of the Load a MIB File dialog box. If the selected MIB file is already present in the database, the MIB file is read, parsed, and loaded from the database. If the MIB file does not exist in the database, MibBrowser parses the MIB file, writes the output to the database, and then loads the MIB file.



The recently loaded MIBs can be loaded automatically at startup by selecting the option, 'Load recently loaded Mibs at startup'.

## Instructions for Using MySQL Database for Loading MIBs

Having tested the loading of MIB files from the MySQL database, you would have understood that the following database parameters have to be configured in the application.

- driver name - org.gjt.mm.mysql.Driver
- url - JDBC: mysql://<machine name>/<database name>
- username - a valid user name
- password - password for the above user

The jar file mysql\_comp.jar has to be included in the CLASSPATH. If the jar is not in the CLASSPATH, the following exception is thrown.

```
Java.lang.ClassNotFoundException:org.gjt.mm.mysql.Driver
```

## Instructions for Using Oracle Database for Loading MIBs

The loading of MIB files from the Oracle database has been tested. The following database parameters are to be configured in the application.

- driver name - org.jdbc.driver.OracleDriver
- url - jdbc:oracle:thin:@<machine name>:1521:<database name>
- username - a valid user name
- password - password for the user

The Oracle driver has to be included in the CLASSPATH. If the jar is not present in the CLASSPATH, the following exception is thrown.

```
Java.lang.ClassNotFoundException:oracle.jdbc.driver.OracleDriver
```

For other databases, use the equivalent parameters.

A few MIB files are provided in the mibs directory, i.e., RFC1213-MIB, RFC1271-RMON, RFC1155-SMI, RMON2-MIB, TOKEN-RING-RMON-MIB, and RFC1315-FRAME. It may be convenient to copy your MIB module files that are to be loaded into the "mibs" directory.



Apparently, MIBs are always parsed before loading when the following operations are performed:

- Loading MIBs directly
- Loading MIB from Compiled File for the first time
- Selecting the "Overwrite existing compiled MIB files" option
- Loading MIB from database for the first time

### 6.15.1.3.2 Unloading MIBs

The next basic MIB operation is unloading. To unload the MIB, select the node of the MIB tree and click the Unload MIB Module button  or select **File-->UnLoad MIB** from the menu. Alternatively, you can press the Delete key.

Performing any of the above prompts you for a confirmation. Selecting 'Yes' unloads the MIB module. If no module is selected in the MIB tree, all the loaded MIB modules are unloaded.

The Load All MIBs option in the menu bar would load all the previously loaded MIBs and Unload All MIBs would unload all the loaded MIBs in the MIB tree.

### 6.15.1.3.3 Parsing MIBs

MibBrowser enables you to parse the given MIB file and check for the macro constructs. It allows different levels of parsing and the parsing is done as per the standard definition of the macros.

The parsing levels can be set in the MibBrowser Settings dialog box. The following table describes the different levels of parsing that can be set and their corresponding checks.

S.No	Level of Parsing	Checks	Description
1	Lenient	No Checks	This level accepts all types of MIB files. For example, it allows both SMIv1 and v2.
2	Normal	Default checks	This level is the default level conforming to the obsolete standards, such as RFC 1902, RFC 1903, etc. Most MIBs follow the obsolete standard.
3	Serious	Most checks throw exceptions on first misbehavior.	This level strictly follows the current standard. It accepts the constructs with inter-operability and implementation problems.
4	Critical	All possible checks throw exceptions on first misbehavior	This level completely follows the SMIv1 and v2 standards. However, it does not accept the backward compatibility constructs, constructs with inter-operability and implementation problems, etc.

Applications, while loading MIB files, perform the following operations:

- Parsing and validating the syntax of the MIB module
- Constructing the MIB module into the tree structure

While performing the parsing and validation of the MIB files, if the MIB modules fail to conform to the SMI standards, the loading will not be done. However, the application requirements might mandate the loading of the non-standard files. On the other hand, some applications might require a stricter check on the compliance with the standards.

The parsing and validating the syntax of the MIB file can be made configurable to suit the application requirements. MibBrowser handles this by providing parsing levels which facilitate to select the level of parsing required by the applications.

In addition to the above four parsing levels, MibBrowser supports another level, which is user-defined. In case of user-defined level, you can define your own parsing level with the required checks at run time.



It is recommended to use the higher parsing level (SERIOUS, CRITICAL) for validating the MIB file and not for loading the MIB file in the application. It affects the performance of the application while loading the MIB files, because it takes considerable amount of time and resources, such as memory, CPU usage, etc.

#### User-Defined Parsing Level

In addition to the four parsing levels, you also have another level, which is user-defined to define your own parsing levels at run time. To add a user-defined parsing level, select the User-Defined option and click the Add button in the User-Defined Levels section. This displays the Customized Level dialog box. Double-click the Levels folder to display a list of all the checks.

By default, all the checks are included. Provide a name for the level in the Level Name text field. To add or remove checks from the level, select or deselect the checks and click OK. Note that if you select (or deselect) a parent check, all its child checks are also selected (or deselected). Click OK to add this level to the user-defined level list.

The level of the parser has to be set in the MibParser before loading a MIB. This level, once set, is used for subsequent MIBs loaded. If the level needs to be modified for the next set of MIBs loaded, it has to be set again in the MIB Parser. In the Mib Settings tab of the MibBrowser Settings dialog box, select the required Parsing level, and click Apply.

The MIB file can contain one or more MIB modules. MibBrowser loads all the dependency files to resolve the MIB module. If the dependency file is not present, the IMPORTS failed error is thrown.

The parsing level can be set for the dependency file by selecting the Import File option and choosing Parsing Levels.

## 6.15.1.4 SNMP Operations

---

- SNMP GET
  - SNMP GETNEXT
  - SNMP GETBULK
  - SNMP SET
- 

MibBrowser allows the user to perform the typical SNMP operations. The operations are categorized as:

- **Retrieving Data** - GET, GETNEXT, GETBULK
- **Altering Variables** - SET
- **Receiving Unsolicited Messages** - Traps

To perform any basic operation as categorized above, it is essential to specify the Object ID, the instance, host name, and the community string. Changes can also be made to the parameters in the MibBrowser Settings dialog box. To get a vivid outlook on the MibBrowser settings, refer to the Configuration topic.

### Specifying the Index

To specify an object to an SNMP agent, both the Object ID (which defines the type of object) and the instance (the specific object of the given type) need to be provided. From the MIB you can get the Object ID, to which an instance needs to be added to completely identify the object of interest.

For non-tabular or scalar objects, the instance is 0. For example, sysDescr is a scalar object under the system group in RFC1213-MIB and it should be specified as sysDescr.0 in Object ID field of MibBrowser. In MibBrowser, this need not be specified if the MIB is loaded, i.e., RFC1213-MIB. MibBrowser adds it to the selected node while performing the GET operation.

For tabular objects, the instance is defined in the MIB as index, and it is a sequence of one or more objects. For example, ifInOctets of ifTable defined in RFC1213-MIB, the index is ifIndex (INTEGER) and may be specified as ifInOctets.1 provided that there exists a row with index 1 in the querying agent.

Another example is tcpConnState of tcpConnTable under tcp group of RFC1213-MIB. The indexes of the tcpConnTable are tcpConnLocalAddress (IpAddress), tcpConnLocalPort (INTEGER), tcpConnRemAddress (IpAddress) , tcpConnRemPort (INTEGER) and may be specified as tcpConnState.179.74.15.126.1192.225.226.126.197.80 provided that there exists a row with Index 179.74.15.126.1192.225.226.126.197.80 in the querying agent where

- 179.74.15.126 represents the value of the first index tcpConnLocalAddress (IpAddress),
- 1192 represents the value of the second index tcpConnLocalPort (INTEGER),
- 225.226.126.197 represents the value of the third index tcpConnRemAddress (IpAddress)
- 80 represents the value of the fourth index tcpConnRemPort (INTEGER).

To get the information about the MIB Node in the MIB Tree, click the Description icon  or choose **View -->Description** menu item or use a shortcut of Alt + R. This gives a list of all the vital characteristics of the node such as the Node, OID, Path, MibModule, Syntax, Status, etc.

## 6.15.1.4.1 SNMP GET

- Performing a Multi-Varbind Request
- Finding MIB Nodes

The GET operation is performed to get one or more values from the managed objects. Follow the steps to perform this operation.

1. Load the MIB file. The loading of MIBs and the options available has been dealt with in detail in the Loading and Unloading MIBs section.
2. Select the desired node in the MIB tree.
3. Click the "Get SNMP Variable" icon  on the toolbar or select **Operations->Get** from the menu bar. Alternatively, you can use the shortcut key combination Ctrl + G.

This operation gets all objects under the selected MIB object, or the specific object if the MIB node and instance are specified.

	<ul style="list-style-type: none"> <li>• If the selected node in the MIB tree has child nodes or columnar nodes, GET operation is performed as an SNMP walk. i.e. the values for all the nodes under that sub-tree are retrieved.</li> <li>• In case, if the MIB is not loaded in the MibBrowser, the exact numbered OID with full instance (for example 1.3.0 for sysUpTime) should be specified and the GET operation should be performed.</li> </ul>
--	---

### Performing a Multi-Varbind Request

To perform the Multi-Varbind request, follow the steps given below:

1. Make the Multi-Varbind display visible in the MibBrowser. This can be made visible by selecting **View-->Display-->Multi-Varbind** from the menu. You can also use the General Settings tab in the MibBrowser Settings panel.
2. Select the leaf node and append the instance by clicking the **Add** button. It will add the OID given in the Object Identifier field and the value given in the SetValue field both separated with a colon to the list. If value is not given in the SetValue field, NULL value is appended. Similarly, you can add as many number of OIDs and values as required.

	Ensure you select the Multi-var check box before doing an SNMP operation for multiple varbind SNMP request. Otherwise, it does a request for the OID in the Object Identifier field.
---	--

3. To delete the varbind(s) from the list, select the varbind(s) from the list and click the **Delete** button.
4. To edit the varbind, select a varbind and click the **Edit** button. It shows an OID and the value of the varbind in the text fields to edit. Edit it and click the **OK** button to modify the OID and value or click the **Cancel** button to restore the old values.

	When the request is sent under Multi-varbind mode, it goes as a single PDU irrespective of the number of OIDs added.
---	--

	If you want to communicate with a v3 agent, you have to select the v3 option in the MibBrowser Settings dialog box and also make sure that the v3 parameters are set. Then perform the above steps for each of the operations.
---	--

## Finding MIB Nodes

You can find a specific node in the MIB tree using the Find dialog box. This is invoked by selecting **Edit-->Find Node** from the menu. Use the Find in All option in the Find dialog box to find a node in all the loaded MIB modules.

### 6.15.1.4.2 SNMP GETNEXT

This operation is similar to the SNMP GET operation, but retrieves the value of the next OID in the tree. This operation is used for traversing the MIB tree. To perform this operation, follow the steps 1 and 2 as in SNMP GET. Then proceed with the following step 3.

3. Click the "Get Next SNMP Variable" button  on the toolbar or select **Operations-->GetNext** from the menu bar. Alternatively, you can use the shortcut key combination Ctrl + N.

This operation will get the next object after the specified object, or the specific object instance, if a MIB node is specified. The instance may or may not be specified. You can also perform a multi-varbind GETNEXT request.

### 6.15.1.4.3 SNMP GETBULK

To retrieve voluminous data from a large table, the GETBULK operation is performed. A GETBULK request is performed by giving an OID along with two other parameters, namely a Max-Repetitions value and a Non-Repeaters value. The GETBULK operation is performed only on SNMPv2c and SNMPv3.

To perform this operation, follow the steps 1 and 2 as in SNMP GET and continue with the following step 3 through 5.

3. Configure the MibBrowser to either SNMPv2c or SNMPv3 as desired. This can be done using either the **Edit-->Settings** option in the menu bar or the MibBrowser Settings icon  on the toolbar. You can also use the shortcut key combination Alt + S. For more details on settings, refer to the Configuration section.
4. Under the same MibBrowser Settings panel, the Max-Repetitions field and the Non-Repeaters field are enabled. The Max-Repetitions value specifies the number of lexicographic successors to be returned for the remaining variables in the variable-bindings list. The default value in this field is 50. The Non-Repeaters value specifies the number of variables in the variable-bindings list for which a single lexicographic successor is to be returned. The default value in this field is 0. Specify the values for these two parameters if you need to and then proceed with the operation.
5. Click the "Get Bulk SNMP data" button or icon  on the toolbar or choose **Operation-->GetBulk** from the menu bar. Alternatively, you can use the shortcut key combination Ctrl + B.

This will get a sequence of Next Objects immediately after the specified object. The number of Object instances returned is equal to the Max-Repetitions field.

## 6.15.1.4.4 SNMP SET

Most network devices have a default value maintained by the agent. Sometimes applications modify the data for one or more MIB variables, thereby using the SNMP SET operation. The following steps will guide you to understand how you can perform the SET operation.

1. Load the MIB file. The loading of MIBs and the options available have been dealt with in detail in the MIB Operations section.
2. Select the desired node in the MIB Tree to which value has to be set. The SET operation can be performed only on the node that has read-write access.
3. Set the value in the Set Value field.
4. Click the "Set SNMP Variable" icon  on the toolbar or select the **Operations-->Set** from the menu bar. You can also use the shortcut key combination Ctrl + W.

### Performing a Multi-Variable SET Operation

To perform the multiple variable SNMP SET request, follow the steps given below:

1. Make the Multi-Varbind display visible in the MibBrowser. This can be made visible by selecting **View-->Display-->Multi-Varbind** from the menu. You can also use the General Settings tab in the MibBrowser Settings panel.
2. Select the nodes in the MIB tree for which the SET operation is to be performed and specify the value to be set for it in the SetValue field.
3. Append the instance by clicking the **Add** button. This adds the OID given in the Object Identifier field and the value given in the SetValue field, both separated by a colon, to the list. Similarly, you can add as many number of OIDs and values as required.



Ensure that the OID and the value that are given in the text fields are correct before you add them to the list.

4. Enable the "Multi-Var" check box present at the bottom and click the **Set SNMP Variable** button on the toolbar. The SET operation is performed on all the nodes added in the multi-varbind list.
5. To delete the varbind(s) from the list, select the varbind(s) from the list and click the **Delete** button.
6. To edit the varbind, select a varbind and click the **Edit** button. It will show an OID and the value of the varbind in the text fields to edit. Edit it and click the **OK** button to modify the OID and value or click the **Cancel** button to restore the old values.



- When the request is sent under Multi-varbind mode, it goes as a single PDU and not as broken PDUs (irrespective of number of OIDs added).
- If you want to communicate with a v3 agent, you have to choose Version3, from the list box in the MibBrowser Settings dialog box and also make sure that the v3 parameters are set. Then perform the above steps for each of the operation.

To perform a SET operation for Octet String Type in hex format, enter the bytes in hex format with each bytes separated by a colon and the entire string within single quotes. For example, to give 0xff0a3212, enter 'ff:0a:32:12' in the Set Value field.



You can find a specific node in the MIB tree using the Find dialog box. This is invoked by selecting **Edit-->Find Node** from the menu. If you want to find a node in all the loaded MIB modules, select Find in All option.

The various values that have to be specified in the Set Value field with respect to the SYNTAX of the Object are given below.

Base Datatypes/ TCs	How to Set the Value			Comments
	Value	Value in HexaDecimal	Value in Binary	
INTEGER/ Integer32	100	'64'h	'1100100'b	For the binary and hex formats, the value should be given within single quotes and should end with b/B and h/H respectively. Note: Binary and Hex values are always unsigned.
Unsigned32	100	'64'h	'1100100'b	
OCTET STRING	adventnet			It accepts all string values.
OBJECT IDENTIFIER	1.3.6.1.2.1.1.1.0 or 1.1.0			It accepts all complete OIDs. if the OID does not start with a dot, the standard prefix ".1.3.6.1.2.1." will be added.
NULL				It creates the SnmpNull object irrelevant to the input you give.
Counter/ Counter32	100	'64'h	'1100100'b	
Counter64	100	'64'h		
Gauge/ Gauge32	100	'64'h	'1100100'b	
BITS STRING				It accepts all the string values.
BITS {zero(0), one(1), two(2), three(3), four(4), five(5) }	1 3 5 / one three five / one 3 five	'54'h/'54'H or 54h/54H '50'h/'50'H or '5'h/50'H	'010101000'b / '010101'b 010101000b / 010101b	The trailing zeros can be omitted. E.g., '50'h the trailing can be used as '5'h
TIMETICKS	100	'64'h	'1100100'b	
IpAddress	192.168.1.220 / hostName			
NetworkAddress	192.168.1.220 / hostName			
OPAQUE		'64'h		It accepts all string values given.
DateAndTime	1995-9-21, 13:53:32.3, -7:0 or 995-9-21, 13:53:32.3	'07:cb:09:15:0d:35: 20:03:2d:07:00' or '07:cb:09:15:0d:35: 20:03'		The value should be 8 or 11 bytes. '07:cb:09:15:0d:35:20:03:2d:07:00' (within single quotes)/ 1995-9- 21,13:53:32.3,-7:0 (11 bytes length) or '07:cb:09:15:0d:35:20:03' / 1995-9- 21,13:53:32.3 (8 bytes length)
TAddress	192.168.1.120 / 161			The value should be 6 bytes The ipAddress and port are separated by a slash.
MacAddress		f1:f2:f3:f4:f5:f6		The value should be 6 bytes. Here, each octet in hex format is separated by colon (:)

## 6.15.1.5 Trap Handling

---

- Viewing Traps
  - Parsing Traps
  - Creating Parser Files
  - Editing Parser Files
- 

The agent, when faced by some problem or error in the transmission of message, responds to the manager by sending unsolicited messages called traps.

Traps are unsolicited messages sent from an SNMP agent to one or more SNMP Management applications. It is an asynchronous notification sent by the agent to the manager about some event occurrence in the device.

In order to receive and view the incoming traps to the specified port, MibBrowser has Trap Viewer.

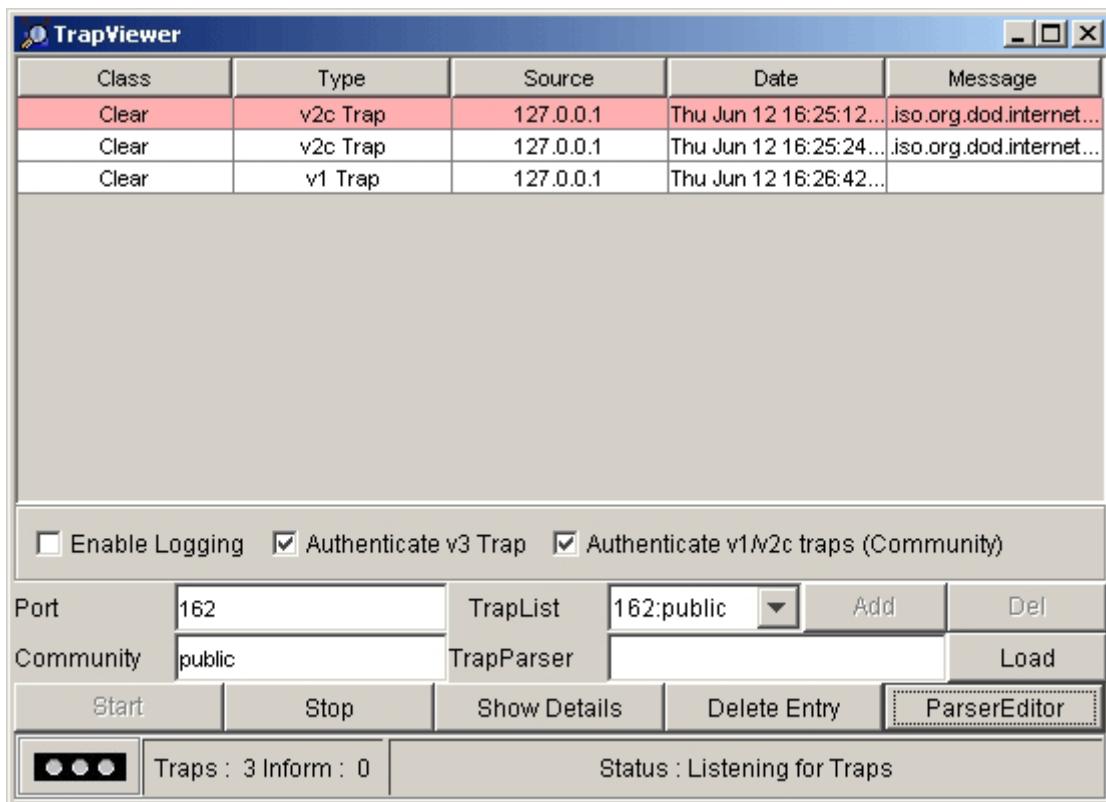
Trap Viewer can be used for viewing and parsing traps. You can also create parser files using the Trap Parser editor and edit them.

## 6.15.1.5.1 Viewing Traps

**Trap Viewer** is a graphical tool to view the traps received from one or more SNMP agents. Trap Viewer can listen to one or more port at a time and the traps can be sent from any host. Trap Viewer can handle inform requests as well. Inform requests can be sent from a manager to another manager. Trap Viewer can receive and display inform messages. By default, the inform requests are sent to the port 162 of the manager station.

To open Trap Viewer, click the Trap Viewer icon on the toolbar or select **View-->Trap Viewer** from the menu. You can also use the shortcut key combination Alt + P.

The image depicted below is a screen shot of Trap Viewer.



Trap Viewer has a table that depicts the trap information and the text fields where the values for common parameters are entered. There are other options, such as Start, Stop, Trap Details, Delete Trap, and ParserEditor.

Follow these steps to know more about the available options.

1. The value in the **Port** text field is set to 162 by default. Enter the desired port in this field.
2. The default value of the **Community** field is public. Set the community of the incoming traps as desired. If you add the community name, The incoming v1 and the v2c traps are validated with the specified community name. If no community name is added, all the v1 and v2 traps with the default community name "public" can be viewed. Also, v3 traps can also be received if the corresponding v3 entry is added. Note that you need not add the community name for receiving v3 traps.
3. Click the **Add** button to add the Port and Community list to the Trap list. This is visible in the **TrapList** list box.
4. The Port and Community list can be deleted by clicking the **Del** button.
5. Click the **Load** button to load the trap parser file.

6. In order to receive the traps now, click the **Start** button. Trap Viewer begins to receive traps from the specified port and community.
7. The traps when received are listed in the **trap table**. The trap table has the following five columns:
  - The **Class** column defines the severity of the trap.
  - The **Type** column defines the type of the trap or the inform request.
  - The **Source** column represents the IP address of the source from where the traps were sent.
  - The **Date** column shows the date and time when the trap was received.
  - The **Message** column has the VarBind list of the trap, if any.
8. The status of the trap is displayed in the status pane at the bottom of the dialog box. Moreover, the Trap count and the inform count is displayed in the status pane.
9. To log the received traps, select the **Enable Logging** check box. All the incoming traps are logged to a file. The default name of the log file is trap.log.
10. Selecting the **Authenticate v3 Trap** check box enables authentication of v3 traps. By default, the authentication is enabled.
11. Selecting the **Authenticate v1/v2c traps** check box enables authentication of v1/v2c traps. If disabled, the community name is not authenticated and all the traps are received. Otherwise, the community name will be authenticated and unauthenticated traps are dropped.



In case of v3 traps, this option enables the authentication and hence unauthenticated traps will be dropped. When set to false, authentication for v3 traps will not be done and all the traps are received.

12. The details of the traps can be viewed by clicking the **Trap Details** button. You can also right-click the trap in the trap table and select 'View Trap Details'.



Note that v3 traps are received only if the corresponding entry is present in the v3 table. Refer Setting Common Parameters for more information on adding v3 entries.

The various details available in the Trap Details frame are listed in the table below.

Trap Details	Description
TimeStamp	This field shows the value stored in the MIB-II sysUpTime variable converted into hours, minutes and seconds. It is a 32-bit unsigned value indicating the number of centiseconds that have elapsed since the (re)start of the SNMP agent and the sending of the trap.
Enterprise	This field shows the OID of the management enterprise that defines the trap message. The value is represented as an OBJECT IDENTIFIER value and has a variable length.
Generic Type	This field shows the value based on the type of trap. The value is categorized and numbered 0 to 6. They are 0-coldStart, 1-warmStart, 2-linkDown, 3-linkUp, 4-authenticationFailure, and 5-egpNeighborLoss. The trap type value 6 is identified as an enterprise-specific value.
Specific Type	This field can have values from 0 to 2147483647. The specific trap type indicates the specific trap as defined in an enterprise-specific MIB. If the Generic Type value is 6, this field shows a value greater than 0. If the Generic Type value is a value other than 6, then the field shows a value 0.
Message	This is a text field. By default, this field always contains the Varbinds in the Trap PDU. This can be replaced with the text.
Severity	This field shows the severity or the intensity of the trap. It could be 0-All, 1-Critical, 2-Major, 3-Minor, 4-warning, 5-Clear, and 6-Info.
Entity	This field contains the source IP address from which the Trap was sent.

Trap Details	Description
RemotePort	This field reveals the port from which the Trap was sent by the originator.
Community	This field contains the Community string.
Node	Source
TimeReceived	This field contains the date and time when the trap was received.
HelpURL	The URL shown here gives more details of the received trap. By default, the URL is <generic-type value> - <specific-type value>.html

13. You can stop listening to the port by clicking the **Stop** button.
14. When you need to delete a trap, select the trap and click the **Delete Trap** button. You can also right-click the trap in the trap table and select 'Delete the Selected Rows'.
15. Another option in Trap Viewer is the **ParserEditor**. Trap Viewer can filter the incoming traps according to certain criterion called the Parser Criteria. The configuration of the criterion is made possible by using the ParserEditor. A detailed overview has been given in the Parsing Traps section.

## 6.15.1.5.2 Parsing Traps

---

- Invoking the Trap Parser
  - Load Trap Parsers and MIB Files
  - Match Criteria
  - OID and Value
  - Agent and Port
  - OutPut Event Parameters
- 

The Trap Parser editor is a tool to create a Trap Parser file. Trap Viewer parses the file created using the Trap Parser editor, with the help of the TrapParserBean, to match each incoming traps with certain criterion. Trap Parsers are required to translate or parse traps into understandable information because traps typically contain cryptic information which is not easily understandable to the users.

The Trap Parser editor:

- configures Trap Parser files.
- parses the traps into an understandable format.

### **Invoking the Trap Parser**

To invoke the Trap Parser editor, click the Parser Editor button in Trap Viewer UI. You can create a new Parser file from an existing Parser file or a MIB file. You also have an option to create a parser file from scratch using the Create Custom Parser File option.

### **Load Trap Parsers and MIB Files**

The next screen of the Trap Parser editor has the options for loading Trap Parser files. The Save option is not enabled when MibBrowser is used as an applet because of the security restrictions. There is also an option for loading MIB files that contain trap definitions.

### **Match Criteria**

Each incoming trap has to possess the Parser match criteria to be shown in the trap table. In the General tab of the next screen, you can enter any number of Parser match criteria into a single parser file with a different parser name. Trap Viewer looks for a match criterion sequentially. Once a criterion is matched for a trap, further checking of match criteria is skipped, and an event is fired to display the corresponding trap entry in the trap table.

While listening to traps, only one parser file can be loaded by Trap Viewer. A parser file can have any number of match criteria. Trap Viewer checks all the criteria in a Trap Parser file sequentially until one criterion matches. The image below depicts the General tab of the Trap Parser editor.

The various match criteria are tabulated below. These are mandatory parameters.

Match Criteria	Description
Generic Type	Each trap has a generic type number. The Generic types are 0-coldStart, 1-warmStart, 2-linkDown, 3-linkUp, 4-authenticationFailure, 5-egpNeighborLoss, and 6-enterpriseSpecific. The number is to be specified for the Trap Parser. The trap is parsed only when the criteria matches. The only exception is that, a trap is parsed even when the generic field is left blank or a negative value is entered in the field.
Specific Type	This field can have an integer value from 0 to 2147483647. If this field is to be matched, the Generic Type must always be enterprise specific.
Enterprise OID	This is the SNMP enterprise identifier in the trap, which is used for unique identification of traps for a particular application. If you specify the OID in this field, the parser is applied only if the trap enterprise field begins with the enterprise field that you have specified. The only exception is that even when the enterprise field is left blank, the trap is allowed to be parsed.

If you had loaded a MIB file or a parser file in the previous screen, the corresponding trap parsers are listed in the Parser List section. You can add, modify, or delete these parsers to create your parser file.

## OID and Value

In the OID tab, you can specify the multiple values in the OID and Value text fields to match. The Trap PDU should match all the OID:Value pairs to conform to this criterion. This criterion extends the matching criterion.

## Agent and Port

In the Agent tab, the trap is sent by an agent, specified in the Agent and Port text fields. If the value of Port is 0, the source can send the trap from any port. The incoming trap must match any of the criteria in the Agent and Port text fields.

## OutPut Event Parameters

For each matching criterion, a trap name is given. The fields in the event details are configured in the Output Event section. Once the trap is matched by the criteria, the trap is added to the Trap Table. The Output Event parameters are shown as the Trap Details, which gives more specific information on the trap.

By default, some of the field of the Output Event parameters are filled by a variable called parser variables usually starting with a "\$". These variables substitute specific characteristics of the parser in the Trap Details.

Each parser variable and its corresponding characteristics are tabulated below.

Variables	Characteristics
\$Community	This token is replaced by the community string of the received trap.
\$Source	This token is replaced by the source name/address of the received trap.
\$Enterprise	This token is replaced by the enterprise ID of the received trap.
\$Agent	This token is replaced by the agent address of the received trap.
\$SpecificType	This token is replaced by the specific type of the received trap.
\$GenericType	This token is replaced by the generic type of the received trap.
\$Uptime	This token is replaced by the up time value in the received trap.
\$*	This token is replaced by all the variable bindings of the received trap, including the OID and values of each variable binding.

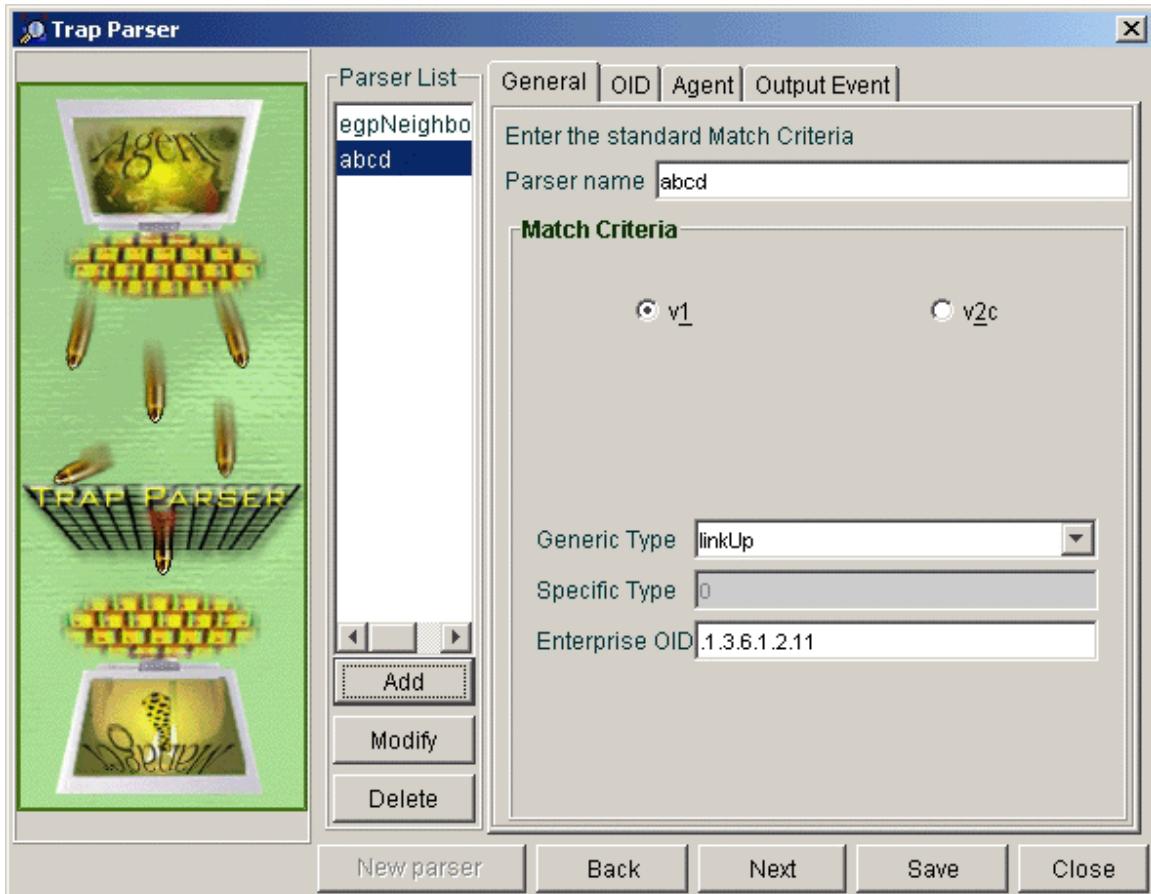
Variables	Characteristics
\$#	This token is replaced by all the SNMP variable values in the variable bindings of the received trap.
\$N	This token is replaced by the (N-1)th SNMP variable value in the variable bindings of the received trap.
@*	This token is replaced by all the OID values in the variable bindings of the received trap.
@N	This token is replaced by the (N-1)th OID value in the variable bindings of the received trap.

### 6.15.1.5.3 Creating Parser Files

- Filtering Traps
- Adding Trap Definition from Any MIB file to a Parser File

A parser file can be created using the Trap Parser editor. Let us now create a Parser file using the Trap Parser editor. Refer to the [Parsing Traps](#) section for invoking Trap Parser and understanding the various parameters available under the Match Criteria.

1. Click the ParserEditor button in the Trap Viewer to invoke Trap Parser.



2. In General tab, enter the values for the Match Criteria parameters as follows.
  - Generic Type: linkUp
  - Specific Type: 0 (because it is a Generic Trap)
  - Enterprise OID: .1.3.6.1.2.11
3. Select the OID tab and enter the following value:
  0. OID/Value (VarBinds): .1.3.6.2.1.1.5.0 xyz

4. Select the Output Event tab. The values depicted for the parameters by default are listed below:
  0. Severity: "-"
  1. HelpURL: "\$GenericType-\$SpecificType.html"
  2. Message: "\$\*"

Change the values to:

  - Severity: Major
  - Message: This is a Message
5. Click the Severity Color button to change the color in which the trap is visible in the trap table.
6. Enter the trap name in the Trap Parser Name field in the Match Criteria section and click the Add button to add the Trap Parser to the Parser list.
7. Add more Match Criteria for the incoming traps and click the Save button to save the current parser criteria. Save the file with the name "test". The Parser filename is displayed in the Parser File text field.
8. Close the Trap Parser editor.

When you need to modify the added Trap Parser, make the changes in the Match Criteria and OutPut Event Parameters, and click the Modify button. It is essential to save the parser file again to effect the changes.

The created Parser file can also be edited manually. Refer to Editing Parser File for more details.

## Filtering Traps

Let us have an overview of filtering of the traps. Follow the steps to perform trap filtering.

1. Click the Load button in the Trap Parser editor to load the Trap Parser file.
  2. Now, send a trap from the applications directory of the AdventNet SNMP API package with the following command.
- ```
java sendtrap localhost .1.3.6.1.2.11 localhost 3 0 1000
```

On receiving the trap, the trap is parsed and checked if it matches the criteria specified in the 'test' parser file. This trap is received because it conforms to the match criteria.

## Adding Trap Definition from Any MIB file to a Parser File

To add a trap definition from any MIB file to a parser file, select the MIB file by clicking the Load button. The parameters are displayed automatically with their respective definitions in the Match Criteria and Output Event parameters sections.

## 6.15.1.5.4 Editing Parser Files

The Parser file created by Trap Parser editor can also be edited using any text editor. When the Parser file is opened in any text editor, the contents of the Parser file would look like this.

```
customMatchDefn=
color=-39424
severity=2
helpDefn=$GenericType-$SpecificType.html
GT=1
ST=0
agentAddressDefn=
enterprise = .1.3.6.1.2.11
textDefn=\ifIndex:\$0\\,rate\=$1
name=a
```

The content of the parser file reveals the various vital parameters of Trap Parser. The table below lists the various parameters and the ways to configure them.

| Parameter        | Configuration                                                                                                                                                                                                                                                                                                                                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| customMatchDefn  | This has the OID:Value pair as the match criteria.<br>Example: .1.3.6.1.2.1.1.1.0:abcd;.1.3.6.1.2.1.1.2.0:acme<br>"\\" is required before ":" for every OID value pair and each pair is separated by a ";"                                                                                                                                                  |
| Color            | This depicts the color of the trap entry in the trap table. The value of the color ranges from -1 to -16777216                                                                                                                                                                                                                                              |
| entityDefn       | This is the machine name from where the trap is originated.                                                                                                                                                                                                                                                                                                 |
| severity         | This field shows the severity or the intensity of the trap. This severity determines how a fault is affected by this event. The type of this filed is an integer ranging from 0 to 6.<br>0 denotes All<br>1 denotes Critical<br>2 denotes Major<br>3 denotes Minor<br>4 denotes Warning<br>5 denotes Clear<br>6 denotes Info.<br>By default, 5 is assigned. |
| helpDefn         | The URL of the document associated with the trap is specified here. By default, it is <generic-type value><specific-type value>.html                                                                                                                                                                                                                        |
| GT               | This depicts the Generic Type trap and the value ranges from 0 to 6.<br>0 denotes coldStart.<br>1 denotes warmStart.<br>2 denotes linkDown.<br>3 denotes linkUp.<br>4 denotes authenticationFailure.<br>5 denotes egpNeighborLoss.<br>6 denotes enterprise-specific.                                                                                        |
| ST               | This is the Specific Type trap. The value can range from 0 to 2147483647.                                                                                                                                                                                                                                                                                   |
| agentAddressDefn | This will contain the agent:port pair, as the match criteria.<br>Example: 127.0.0.1:0;192.168.1.2:0<br>"\\" is required before ":" for every agent port pair and each pair is separated by a ";"                                                                                                                                                            |
| enterprise       | This is the enterprise OID of the trap.                                                                                                                                                                                                                                                                                                                     |
| textDefn         | This is the message text for this event in the ListTraps and logs.                                                                                                                                                                                                                                                                                          |
| Name             | The name of the parser is given here.                                                                                                                                                                                                                                                                                                                       |

## 6.15.1.6 Table Handling

---

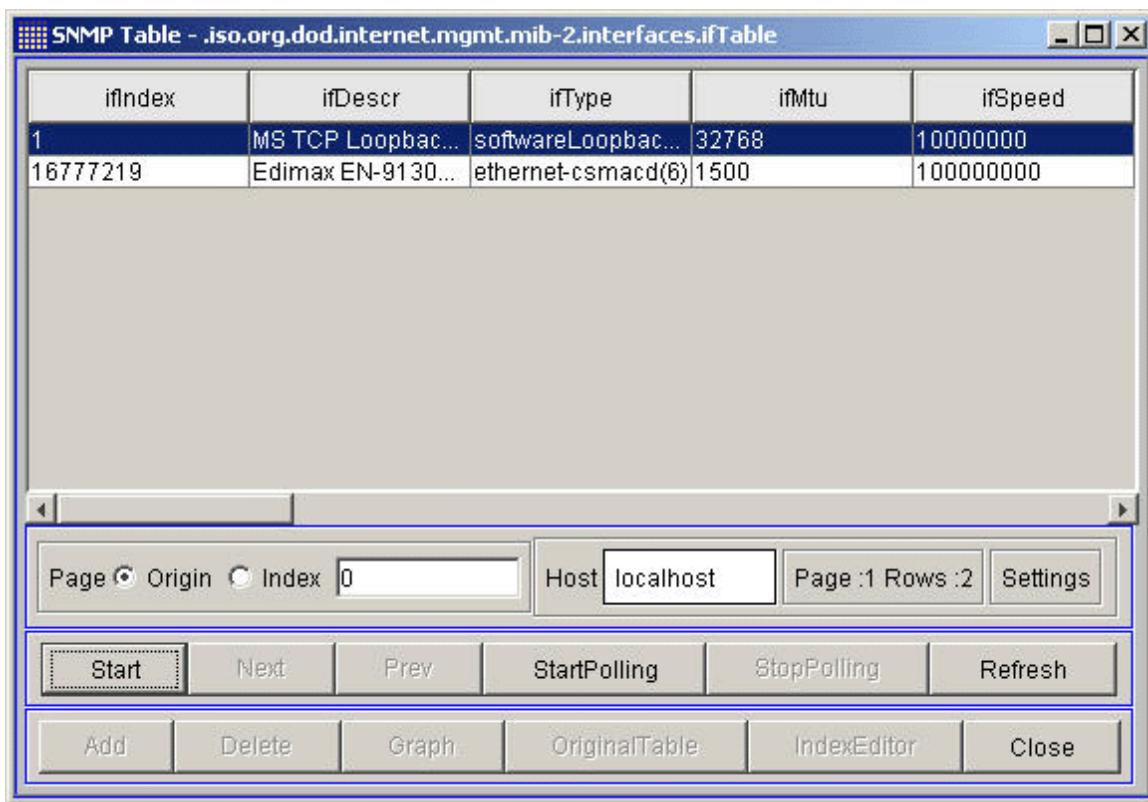
- Retrieving Table Data
  - Adding Rows
  - Deleting Rows
- 

AdventNet MibBrowser enables you to view the SNMP Table data in a separate window called the SNMP Table Panel. The table has a very user-friendly profile. The SNMP Table panel has various options using which you can add and delete rows, view graphs, and use index editor.

## 6.15.1.6.1 Retrieving Table Data

The data in the table can be retrieved with ease. The following steps gives you an insight into how to open the Data Table panel and work on it using the various options.

1. Specify the proper agent host name or IP address in the Host field of MibBrowser.
2. Load the MIB file in MibBrowser. To know more on Loading the MIB file, refer to the Loading and Unloading MIBs section.
3. Specify a valid OID or select the OID by traversing through the Mib Tree. The OID should be a valid table OID.
4. Click the **View SNMP data table** button  on the toolbar or choose **View-->Snmp Table** from the menu. You can also use the shortcut key combination Alt+T.
5. This would invoke the SNMP Table of the specified table OID. The figure below depicts the SNMP Table panel.

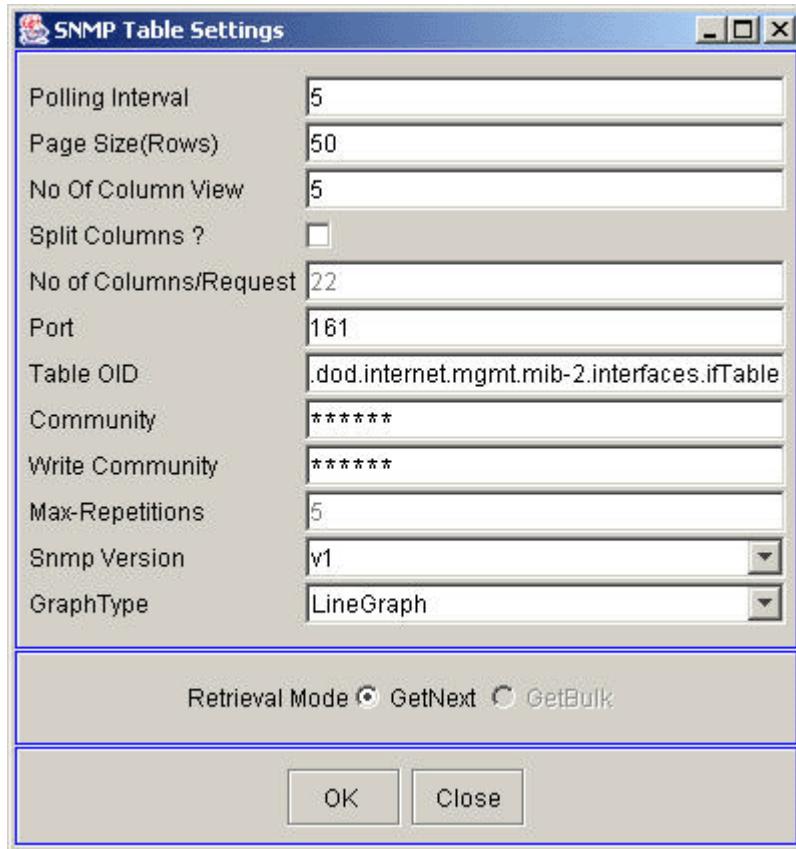


| ifIndex  | ifDescr           | ifType             | ifMtu | ifSpeed   |
|----------|-------------------|--------------------|-------|-----------|
| 1        | MS TCP Loopbac... | softwareLoopbac... | 32768 | 100000000 |
| 16777219 | Edimax EN-9130... | ethernet-csmacd(6) | 1500  | 100000000 |

Click the **Start** button at the bottom of the SNMP Table panel. The retrieval of data begins and the columnar objects are obtained and displayed in the table.

6. Click the **StartPolling** button to start the polling of the table. The polling interval is based on the Polling Interval value set using the Settings option.
7. Click the **StopPolling** button to stop the polling.
8. When you don not use the polling option, click the **Refresh** button to refresh the table.
9. The SNMP Table panel might retrieve more data so that the frame depicting the columnar objects would run to pages. When you need to navigate through the pages (rows), use the **Next** and **Prev** button.
10. The **Page** option at the bottom of the panel is used to specify how the table retrieval needs to be done. If the option is origin, the table is retrieved from the origin. If the option is index, the user can set an index value from which the table can be retrieved.

11. The host name as specified in MibBrowser will be displayed in the Host field. The page number and the number of rows in that page are displayed next to it.
12. It is possible to configure the SNMP Table panel. Click the 'Settings' button. This displays a dialog box with various options to configure the Table panel. The image below depicts the SNMP Table Settings panel.



The various options available are listed below:

- **PollingInterval** - This specifies the time interval between each retrieval of data. The default value is 5 secs.
- **Page Size (Rows)** - The number of rows to be retrieved is set here. The default value is 50.
- **No Of Column View** - This specifies the number of columns to be displayed in the SNMP Table panel. The default is 5.
- **Split Columns** - When the size of the PDU exceeds the limit, the agent sends the error message "Too Big PDU Error". This field serves as an option for splitting the PDU. By default, the PDU is split into half. If the number of varbinds is set by the user, then multiple request with PDU containing number of varbinds set is sent.
- **No of Columns/Request** - This field is enabled on selecting the Split Columns check box. You can specify the number for splitting of columns.
- **Port** - This field specifies the port to which the request is made.
- **Table** - The table OID is specified here.
- **Max-Repetitions** - This value specifies the number of lexicographic successors to be returned for the remaining variables in the variable-bindings list. The default value is 5. This is enabled only when the Retrieval Mode option is set to GetBulk.
- **SnmpVersion** - This gives the option to switch to any of the three versions of SNMP-v1, v2c, and v3.

- **Graph Type** - This gives the option to switch between Line Graph and Bar Graph.
  - **Retrieval Mode** - By default, GETNEXT is enabled. The GETBULK option is enabled only on selecting v2c or v3.
2. If you need to view the graph, click the button. The section on Graphs gives you more details on the MibBrowser Graph component.
  3. You can also add and delete rows in the table and a detailed explanation has been given in the next two sections.
  4. In a table, if one of the index columns is an external index, i.e., the index value is shared by some other table, then the table is called an Augmented table. Augmented table comes into picture when there is a one-to-one dependency between rows of two tables. This situation might arise when a particular MIB imports another MIB and shares a single table. For example, ifXTable defined in IF-MIB is an augmented table, which has an external index ifIndex augmented from ifTable. Clicking the 'Augmented Table' button shows the columns of the table which augments the index from the original table.
  5. Click the Index Editor button to edit the index and view the rows from corresponding index.
  6. To make changes to a particular column values, right-click the columns. The various options available are
    - **view column node details** - This option gives the MibNode Information of the selected column.
    - **edit the header name for selected column** - This invokes a dialog box in which you can change the header for the selected column.
    - **view graph for selected cell(s)** - This option invokes the graph. It is possible to view the graphical representation for more than one cell by multiple selection of desired cells.
    - **add a new row to the table** - This option is the same as the Add option available in the Table panel. A detailed overview of adding a row is given in the Adding a row section.
    - **delete the selected rows from** - This option is the same as the Delete option available in the Table panel. A detailed overview of deleting a row is given in the Deleting a row section.
    - **view the not-accessible index** - A request cannot be sent to an index that is not accessible. In the table, the not-accessible index is not visible. Selecting this option would enable you to view the not-accessible index values.

## 6.15.1.6.2 Adding Rows

---

- SMIv1 Tables with entryStatus Column
  - SMIv2 Tables with rowStatus Column
- 

To add a new row to an SNMP table from the manager, the table should be an SMIv1 table with entryStatus defined or an SMIv2 table with rowStatus defined.

### **SMIv1 Tables with entryStatus Column**

The entryStatus column is used to manage the creation and deletion of conceptual rows in SMIv1 tables. This represents the status of a table entry. The status column can have the following:

- 'valid(1)' - indicates that the row exists and is available for use.
- 'createRequest(2)' - supplied by the manager wishing to create a row.
- 'underCreation(3)' - indicates that the row is created.
- 'invalid(4)' - supplied by the manager wishing to invalidate the corresponding entry.

If a manager wishes to add a row, the status column should be set to createRequest(2). Immediately after the creation, the agent sets this object to underCreation(3). The entry remains in the underCreation(3) state until it is configured. Then its value is set to valid(1). If the status remains underCreation(3) for an abnormally long period, the agent sets the status to invalid(4).

### **SMIv2 Tables with rowStatus Column**

In SMIv2 tables, the rowStatus column is used to manage the creation and deletion of conceptual rows. This column has six defined values as follows:

- active(1) - indicates that the conceptual row with all columns is available for use by the managed device.
- notInService(2) - indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device.
- notReady(3) - indicates that the conceptual row exists in the agent, and one or more required columns in the row are not instantiated.
- createAndGo(4) - supplied by a manager wishing to create a new instance of a conceptual row and make it available for use.
- createAndWait(5) - supplied by a manager wishing to create a new instance of a conceptual row but not making it available for use.
- destroy(6) - supplied by a manager wishing to delete all the instances associated with an existing conceptual row.

An existing conceptual row can be in any one of the three states, 'notReady', 'notInService', or 'active'. If the manager wishes to add a row in a single shot with values for all the columns, the status column should be given as 'createAndGo(4)'. After the creation of a row, its value is set to active(1). If a row has to be created with values for only some columns, the status column should be 'createAndWait(5)'. Also, this row with partially filled columns has the status 'notReady(3)'. The entry remains in this state until the values for all the columns are set. After all the values are set, the agent changes this value to active(1).

For SMIv2 tables, a new row can be added in three ways:

- CreateAndWait
- CreateAndGo using Multiple-Variable Set
- CreateAndGo using SNMP table UI

### **CreateAndWait**

In this method, you should SET the RowStatus with value "CreateAndWait", set each column one by one, and finally, set the RowStatus to "Active".

Each SET method can be performed either using MibBrowser or through command line application.

### **CreateAndGo Using Multiple-Variable Set**

Instead of using multiple SET methods to create a new row, you can use Multiple-variable SET method to create a new row in a single SET method. For this, all the columns with their value should be given and RowStatus should be CreateAndGo.

Multiple-variable SET can be done using the command line application.

### **CreateAndGo Using SNMP Table**

A new row for a table can also be created using SNMP table User Interface. The following image displays the SNMP Table dialog box.

Select "add a new row to the table" to invoke the following dialog box. The user has to fill in all the information and click the OK button.



### 6.15.1.6.3 Deleting Rows

To delete a row from an SNMP table from the manager, the table should be an SMIv1 table with entryStatus defined or an SMIv2 table with RowStatus defined.

Using the SNMP table User Interface, you can delete a row from the table. Refer to the following image for more information.

The screenshot shows the "SNMP Table - .iso.org.dod.internet.private.enterprises.adventnet.products.agent.trapModule.forwardingTable" window. The table has four columns: id, managerHost, managerPort, and rowStatus. A dropdown menu is open over the rowStatus cell for the first row (id 1). The options in the dropdown are: active(1), active(1), notInService(2), notReady(3), createAndGo(4), createAndWait(5), and destroy(6). Below the table is a toolbar with buttons for Page, Origin, Index, Host, Start, Next, Prev, StartPolling, StopPolling, Refresh, Add, Delete, Graph, OriginalTable, IndexEditor, and Close.

| id | managerHost | managerPort | rowStatus                                                                                                    |
|----|-------------|-------------|--------------------------------------------------------------------------------------------------------------|
| 1  | managerHost | 1           | active(1)<br>active(1)<br>notInService(2)<br>notReady(3)<br>createAndGo(4)<br>createAndWait(5)<br>destroy(6) |

## 6.15.1.7 Graphs

---

- Line Graph
  - Bar Graph
- 

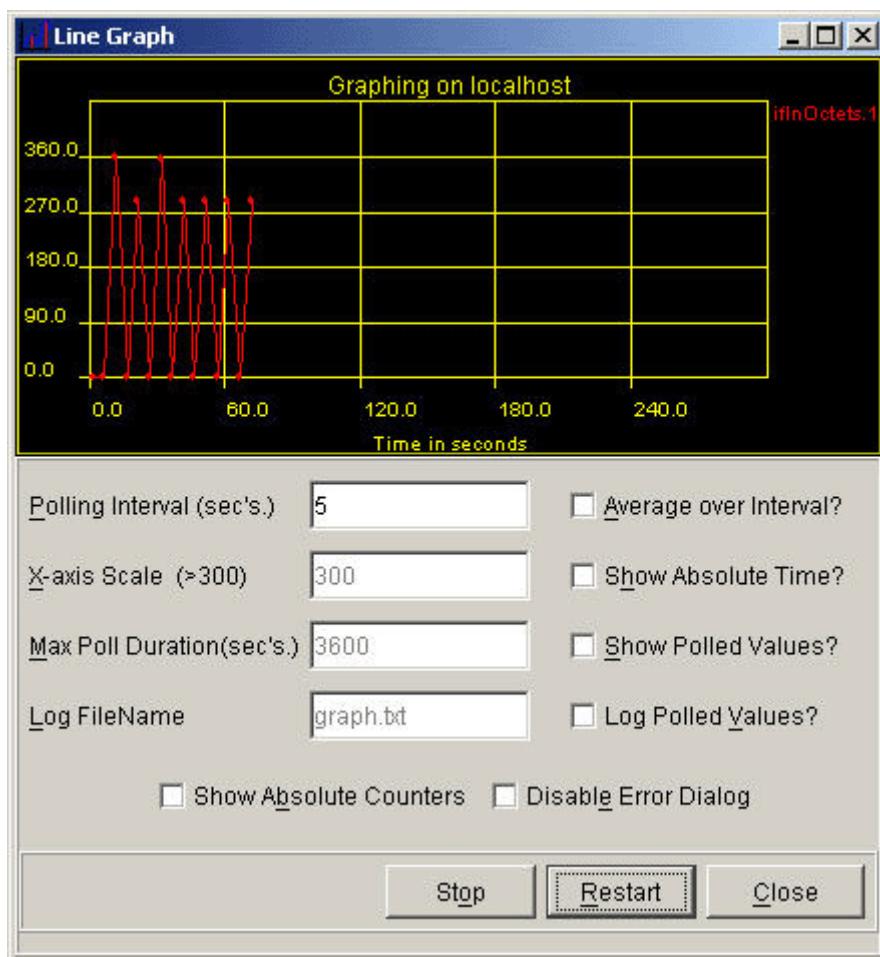
One of the vital features of the AdventNet MibBrowser is the Graphs. The graphs depict the real-time plotting of the SNMP data. Currently, two types of graphs are supported - line graph and bar graph. The SNMP data to be polled should be of integer or unsigned integer data type. Typically, the values that are plotted will be of type Counter, Gauge, or Timeticks.

### 6.15.1.7.1 Line Graph

The Line graph depicts the real-time plotting of the SNMP data. Follow the steps below to invoke a line graph.

1. Specify the proper agent host name or IP address in the Host field of MibBrowser.
2. Load the MIB file in MibBrowser. To know more on loading MIBs and other features associated with it, refer to the Loading MIBs section.
3. Specify a valid variable. The variable must be an integer or unsigned integer (Counter, Gauge, Timeticks). This variable can be entered directly in the variable field or it can be chosen by browsing through the MIB tree.
4. Click the 'View real-time graph' button in the toolbar or select View-->Line Graph from the menu. You can also use the shortcut key combination Alt+L. By default, the line graph is invoked.
5. The updated Line graph shows the results of periodically polling the agent for the specified OID.

The image below depicts a Line Graph invoked from MibBrowser.

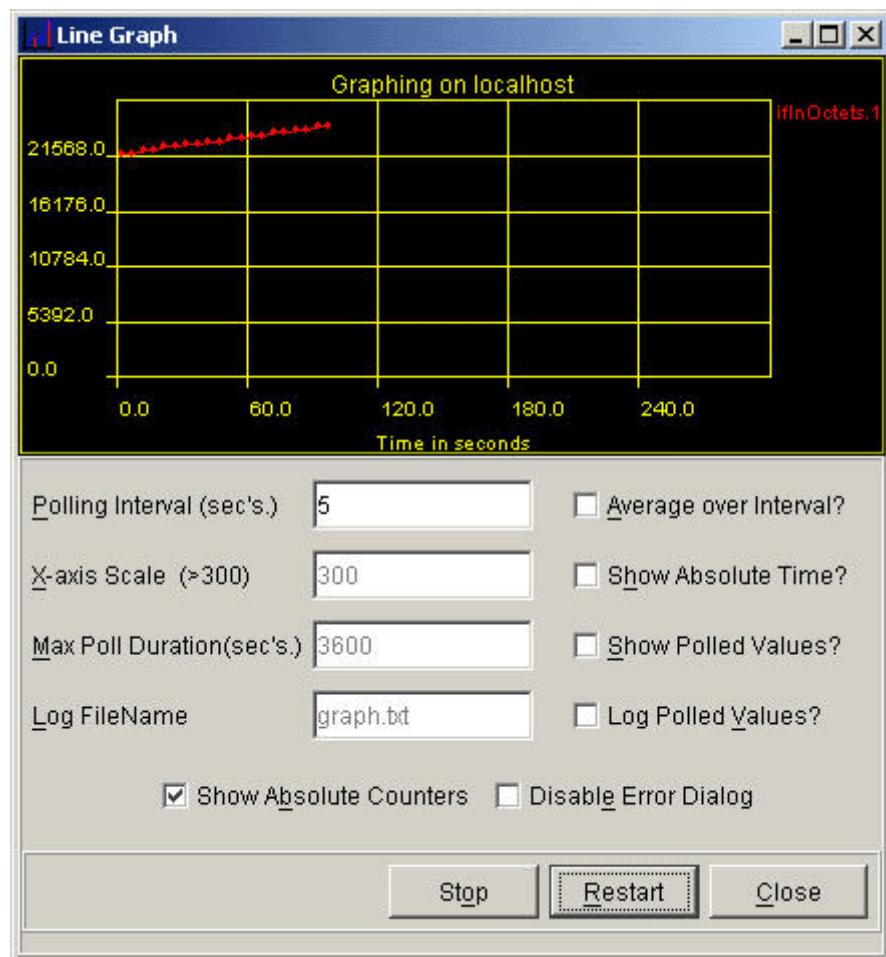


When you move the cursor over the graph, a box containing the current time and values is displayed. The various options available in the Line graph are tabulated below.

| Option                 | Description                                                                                                                                                                                                                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polling Interval       | This specifies the polling interval time. The default value is 5 secs. You can change the interval time as desired.                                                                                                                                                                                             |
| Average over Interval  | By default, the graph shows the actual values of a variable for different hosts. In other words, the values of the specified OID are plotted for different hosts for the given polling interval. Selecting this option, the average of the values at a given polling interval are taken for plotting the graph. |
| X-axis Scale           | This specifies the X-axis scale. The minimum value is 300 secs and this is the default value. Changing this would alter the X-axis scale of the table. This option is enabled only on clicking 'Show Polled values' option.                                                                                     |
| Show Absolute Time     | By default, the time is depicted in the graphs only as seconds. Selecting this option would give you the time in hours:secs.                                                                                                                                                                                    |
| Max Poll Duration      | This option is used to view all the polled values in a particular time period. It is enabled only on clicking 'Show polled values' option. The default value is 3600 secs.                                                                                                                                      |
| Show Polled Values     | This option is used to display all the polled values in a particular period of time. By default, this option is disabled. Only on selecting this option, the Max Poll Duration option is enabled.                                                                                                               |
| Log FileName           | The filename for the log file can be set here. By default, the log filename is graph.txt. If "Log Polled Values" is selected, all the polled values are logged in this file. This option is not enabled when the MibBrowser runs as an applet because of security restrictions.                                 |
| Log Polled Values      | Selecting this option would log the polled values. This would enable the option Log FileName.                                                                                                                                                                                                                   |
| Show Absolute Counters | By default, the graph plots only the difference between the two Counter values. On selecting this, the plotting of the absolute value is performed.                                                                                                                                                             |
| Disable Error Dialog   | Selecting this option would stop displaying the error messages that pop up when a request times out.                                                                                                                                                                                                            |
| Restart                | The Restart button is used to restart the polling.                                                                                                                                                                                                                                                              |
| Stop                   | The Stop button is used to stop the polling.                                                                                                                                                                                                                                                                    |
| Close                  | The Close button is used to close the graph window.                                                                                                                                                                                                                                                             |

Another way of invoking a graph is through the Table options. For a detailed overview on Table Handling and invoking a graph from the table window, refer to the Table Handling section.

MibBrowser can plot multiple graphs showing values for different variables from different hosts. The image below shows the plotting of multiple graphs and with the option 'Show Absolute Counters' enabled.



## 6.15.1.7.2 Bar Graph

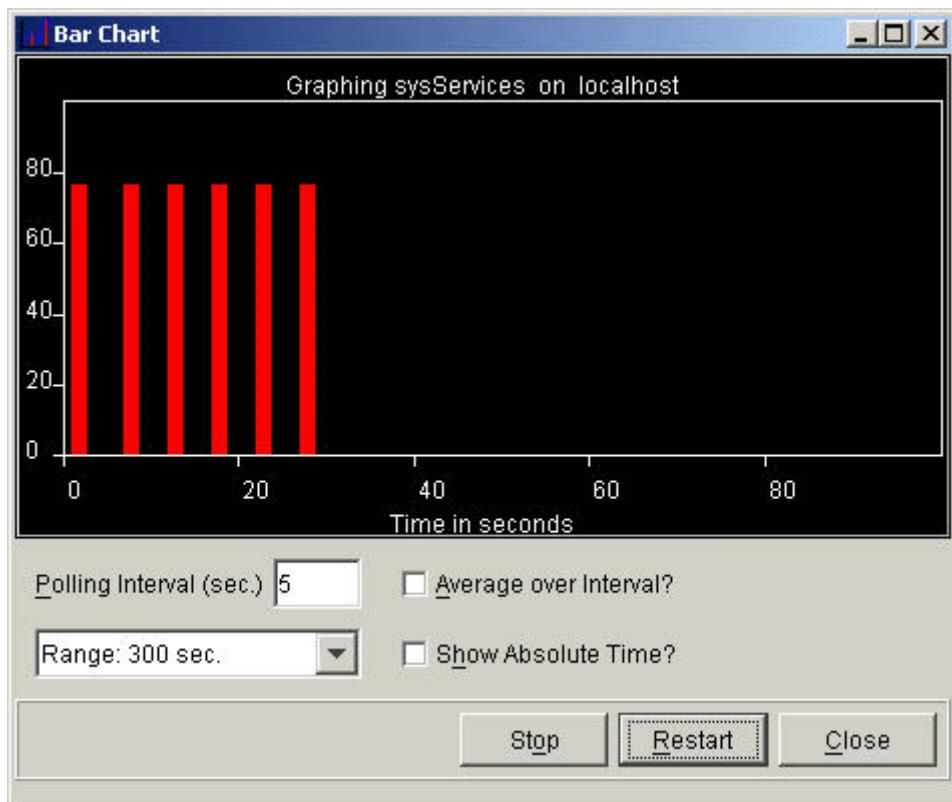
The Bar graph depicts the real-time plotting of the SNMP data. Follow the steps below to invoke a bar graph from the MibBrowser, which is similar to invoking a Line graph.

1. Specify the proper agent host name or IP address in the host field of the MibBrowser.
2. Load the MIB file in MibBrowser. To know more on loading MIBs and other features associated with it, refer to the MIB Operations section.
3. Specify a valid variable. The variable must be an integer or unsigned integer (Counter, Gauge, TimeTicks). This variable can be entered directly in the variable field or it can be chosen by browsing through the MIB tree.
4. Select the **View-->Bar Graph** from the menu bar. You can also use the shortcut key combination Alt + B.
5. The updated Bar graph shows the results of periodically polling the agent for the specified OID.



The Bar graph does not have an option for plotting multiple variables in the graph. Therefore, in case of a columnar OID, you need to append the instance of the index to enable the plotting of Bar graph. For example, to plot a bar graph for the values of the first row of the columnar OID ifOperStatus (ifTable), you need to first select the node ifOperStatus. Then, in the Object ID text field, append ".1" with the OID and select **View-->Bar Graph** from the menu. This plots the value of the first row of the column ifOperStatus.

The image below depicts a Bar graph invoked from MibBrowser.



The various options available in the Bar Graph are tabulated below:

| <b>Option</b>         | <b>Description</b>                                                                                                                                                                                                                                                                                             |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polling Interval      | This specifies the polling interval time. The default value is 5 secs. You can change the interval time as desired.                                                                                                                                                                                            |
| Average over Interval | By default, the graph shows the actual values of a variable for different hosts. In other words, the values of the specified OID are plotted for different hosts for the given polling interval. Selecting this option, the average of the values at a given polling interval is taken for plotting the graph. |
| Range                 | Altering the range would change the X-axis scale of the table. The default value is 300 secs. The other options are 600 secs and 1000 secs.                                                                                                                                                                    |
| Show Absolute Time    | By default, the time is depicted in the graphs only as seconds. Selecting this option would give you the time in hours:mins:secs.                                                                                                                                                                              |
| Restart               | The Restart button is used to restart the polling.                                                                                                                                                                                                                                                             |
| Stop                  | The Stop button is used to stop the polling.                                                                                                                                                                                                                                                                   |
| Close                 | The Close button is used to close the Bar graph window.                                                                                                                                                                                                                                                        |

## 6.15.1.8 Internationalization

AdventNet MibBrowser supports Internationalization. This allows using the MibBrowser application and applet in various languages without changing the source code. Localized content can be added easily and the same executable can be run worldwide. All the textual elements such as GUI component labels and messages can be made suitable to the locale (combination of specific language and country) of the user.

The following are the steps involved in enabling the Internationalization support to AdventNet MibBrowser.

1. The **MibBrowser.properties** file available in the <MibBrowser> directory is to be used as the template file. This file contains the English strings of all the GUI labels and the messages.
2. The **MibBrowser.properties** file has to be copied to the specified locale file. For example, to display the MibBrowser in French language, the **MibBrowser.properties** file is to be copied as **MibBrowser\_fr\_FR.properties** file. The language and the country are to be represented by the standard two-letter codes (fr - French and FR - France). If the specified locale file is not present in the specified directory, the default properties file **MibBrowser.properties** is searched and loaded.
3. The developer has to write the equivalent strings of the chosen language and country in this file. This will enable the MibBrowser to print the user-written strings instead of English strings. For all the strings for which corresponding locale-specific strings are not given, English strings are used.



The format given in the **MibBrowser.properties** file should not be altered. The English strings are provided with the "escape" sequence characters. For example, the string "Save MibBrowser Results As...." is provided as "Save\ MibBrowser\ Results\ As... ". However, the equivalent strings (of the chosen language) need not have the "escape" sequence included. For example, the equivalent string for "Save\ MibBrowser\ Results\ As... ". can be given as "my own language equivalent of the same text".

4. After the above steps, the following code changes have to be done in the **MibBrowserApplication.java**. Before instantiating MibBrowser, the locale has to be set and the font which was supported for the specified locale should be set. For example, to set the internationalization for the French language, you need to include the following (provided that the font 'Helvetica' supports French).

```
MibBrowser.internationalize(new Locale("fr", "FR"), new
Font("Helvetica", Font.PLAIN, 12));
```

The properties file should also be edited with proper French words and copied as **MibBrowser\_fr\_FR.properties**. The properties file should be present in the directory in which the application is executed. If the properties file is present in some other directory, it can be specified by using the static method **setSearchPath()** in the SnmpUtils class.

```
SnmpUtils.setSearchPath(<path of the properties file>);
MibBrowser.internationalize(new Locale("fr", "FR")), new
Font("Helvetica", Font.PLAIN, 12));
MibBrowser mibrowser = new MibBrowser();
```

For applets, similar changes have to be done in the **MibBrowserApplet.java** file. In case of applets, if the properties file is present in any other directory, it can be specified by giving the path related to the document base in the **setSearchPath()** method.

For example, if the document base is /home/test/mibbrowser, the server base is /home/test/ and the properties file is present in the directory /home/test/properties/, the search path should be set as follows:

```
SnmpUtils.setSearchPath("../properties");
```

```
MibBrowser.internationalize(new Locale("fr", "FR")), new  
Font("Helvetica", Font.PLAIN, 12));  
MibBrowser mibrowser = new MibBrowser(applet);
```

5. The Java files have to be compiled and regenerated to reflect these changes.

To implement internationalization in MibBrowser using the default properties file **MibBrowser.properties**, you need to include the following:

```
MibBrowser.internationalize(new Locale("", ""), new  
Font("Helvetica", Font.PLAIN, 12));
```

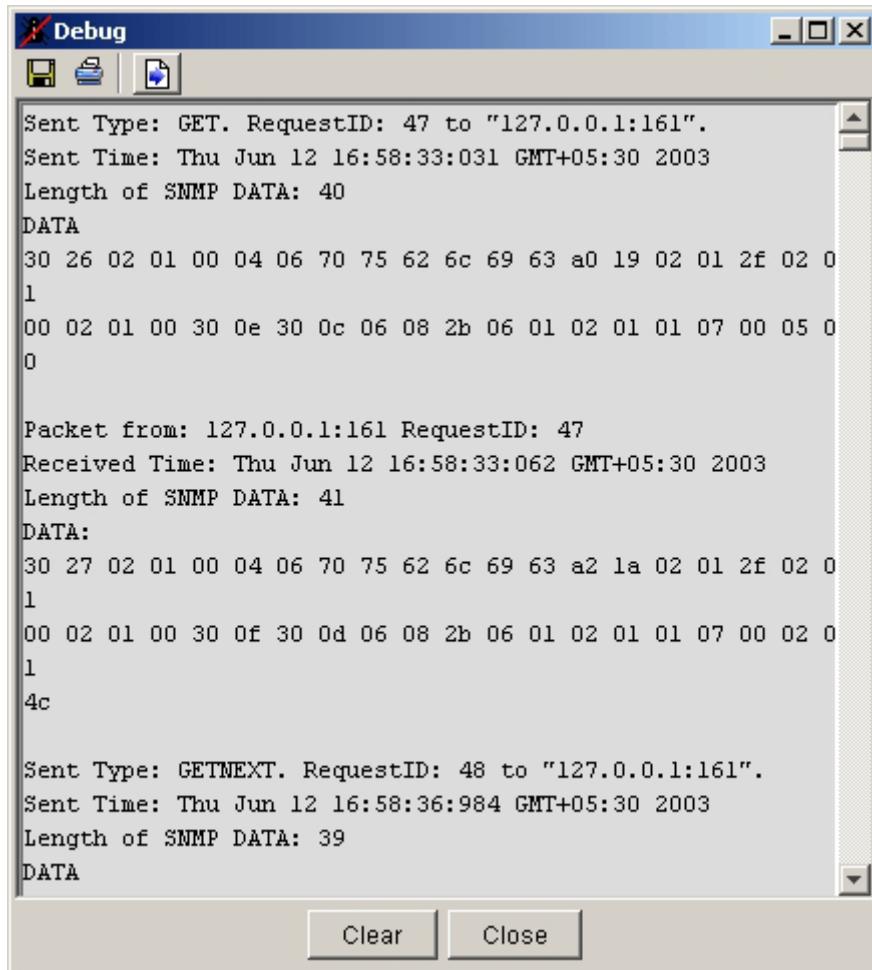
## 6.15.1.9 Debugging and Decoding

The MibBrowser application provides facility to view the debug output of the SNMP operations. The Debug window is used to show the PDU that is sent from the manager and the response PDU that is got from the agent.

### Invoking the Debug Window

1. Click the Debug icon  in the toolbar or select View-->Debug from the menu bar. You can also use the shortcut key combination Alt + D. This would invoke the Debug window.
2. As long as this Debug window is opened, debugging is turned on and the debugging output is displayed. When this window is closed, debugging is turned off.

The image below depicts a Debug window.



3. The three icons in the debug window provide the following functions:
  - Save MibBrowser Debug Results - Saves the debug information to a file.
  - Print MibBrowser Debug Results - Prints the debug information to a file.
  - Snmp Decoder - Switches over to the Decoder window.

The Clear button clears the debug information and the Close button closes the Debug window.

## Invoking the Decoder Window

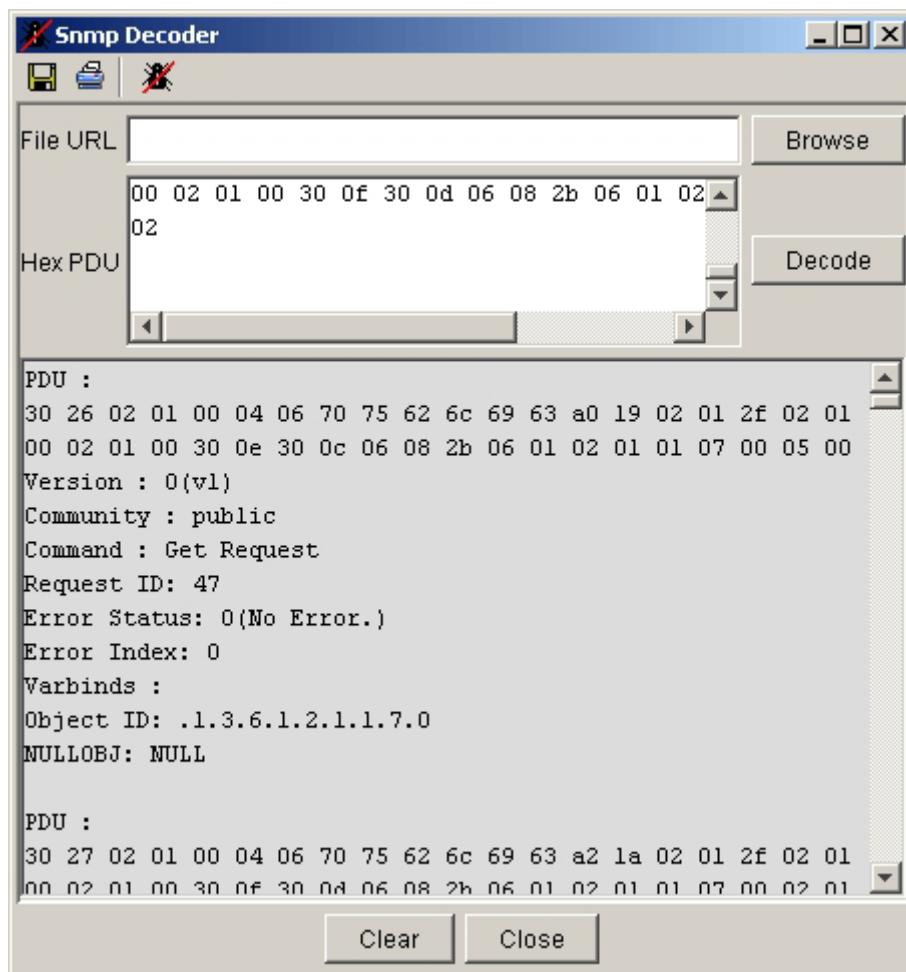
1. To switch over from the Debug window to the Decoder window, click the Decoder icon. The Decoder icon toggles to a Debug button.
2. The three icons in the Debug window provide the following functions:
  - Save MibBrowser Decoder Results - Saves the debug information to a file.
  - Print MibBrowser Decoder Results - Prints the debug information to a file.
  - Debug - Switches over to the Debug window.



The Save and Print options are available only when the MibBrowser is invoked as an application and not as an applet because of security restrictions.

## Performing the Decoding Operation

The Snmp Decoder is used to decode the SNMP debug messages. The figure below depicts the SNMP Decoder.



To decode the debug information, select the PDU in the debug window and click the Snmp Decoder icon. This will switch over to the decoder window. Now, the selected debug information is available in the "Hex PDU" text area. Click the Decode button to decode the information. The decoded message is displayed in the bottom panel of the Decoder window.

If the debug message was stored in a file, the decoding can be done by loading the file. This can be done by clicking the Browse button in the Debug frame. You can also enter the URL in the File URL

text field and press the 'Enter' key. However, saving and loading of debug information files is done only in applications and not in applets.

You can select the entire PDU debug message displayed in the Debug window with all the strings and click the Decoder button to display the selected information in the Hex PDU text area. You can also save the debug message in the Debug window and load it in the Decoder window. The decoder will decode all the PDU dumps leaving the informative strings. The limitation in this is that the two continuous PDUs should have a string delimiter as a new line in between them.

A sample PDU is depicted below.

30 26 02 01 00 04 06 70 75 62 6c 69 63 a0 19 02 01 04 02 01  
00 02 01 00 30 0e 30 0c 06 08 2b 06 01 02 01 01 05 00 05 00

**Packet from: 192.168.1.215 : 161**

**DATA:**

**30 2e 02 01 00 04 06 70 75 62 6c 69 63 a2 21 02 01 04 02 01  
00 02 01 00 30 16 30 14 06 08 2b 06 01 02 01 01 05 00 04 08  
4b 41 4e 4e 41 4e 4b 41**

The highlighted strings will be the delimiter between the two continuous PDU dumps. In case there is no string delimiter as above, only the first PDU is decoded. You can also save the decoded information using the Save button. The Save button in the Debug view saves the debug information.



## 6.151.10 Error Messages

The following is the list of MibBrowser related Error Messages and the different scenarios at which they will be displayed:

| S.No. | Error Message                                                                                                                       | When it is displayed                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | No ObjectID Specified.                                                                                                              | OID is not specified before making a request.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 2     | No Host Specified.                                                                                                                  | HostName is not specified before making a query.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 3     | Host Name Should Be Entered.                                                                                                        | SnmpTable is started without specifying the host name.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 4     | Invalid OID Format                                                                                                                  | The specified OID is not a valid one. Before making any query, Invalid OID Format exception is thrown.<br>It should be either Integer type or String type.<br>It will be thrown during instantiating Line/Bar Graph, SnmpTable, and operations, such as GET, GETNEXT, GETBULK, SET, etc.                                                                                                                                                                                       |
| 5     | Invalid Table OID                                                                                                                   | SnmpTable is started after specifying an invalid OID in the OID Textfield.                                                                                                                                                                                                                                                                                                                                                                                                     |
| 6     | Table OID should be specified                                                                                                       | SnmpTable started without specifying any Table OID                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 7     | Error Loading MIB: xyz<br>java.io.FileNotFoundException:<br>Could not Open stream for<br>home/..../AdventNet/SNMPv3/mibs/xyz.parser | Invalid file is loaded in the LoadMibDialog TextField for loading MIBs File.<br>But in the description TextField of MibBrowser, the message thrown is "Loading Mibs: xyz"                                                                                                                                                                                                                                                                                                      |
| 8     | RequestFailed: Error: Request TimedOut To LocalHost                                                                                 | The error message is thrown when doing the operations such as GET, GETNEXT, and SET and for creating SnmpTable, LineGraph or BarGraph window. <ul style="list-style-type: none"> <li>1. If the agent does not implement the OID that is queried.</li> <li>2. If the agent queried is not present in the network.</li> <li>3. If the port number set is not valid for the agent queried.</li> <li>4. If the Community and Write Community specified are not correct.</li> </ul> |

| S.No. | Error Message                                                                                                                                             | When it is displayed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                                                                                                           | <ul style="list-style-type: none"> <li>5. If the OID queried does not contain any data.</li> <li>6. If for v3 agents security parameters are not set.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 9     | RequestFailed: Get Response PDU received from 192.168.1.001<br>Error Indication In Response: There is no such variable name in this mib.<br>ErrIndex:<br> | <p>The error message is thrown when doing set operation</p> <ul style="list-style-type: none"> <li>1. If, the OID is not instrumented by the agent for which it is setting value.</li> <li>2. If the agent queried is not present in the network.</li> <li>3. If the WriteCommunity specified is not right one.</li> <li>4. If the Syntax of the value you are setting is not as that required by the OID.</li> </ul> <p>The same Exception is also thrown when plotting Graph for a leafNode is not instrumented by the agent for which it is setting value.<br/> And also when querying for data in an SnmpTable</p> <ul style="list-style-type: none"> <li>1. If data is not available.</li> </ul> |
| 10    | RequestFailed: Get Response PDU received from 192.168.1.001<br>Error Indication In Response: A not writable error occurred.<br>ErrIndex: 1                | The leafNode or OID for which you are setting value has no read/write access.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 11    | Error Sending Set Request : com.adventnet.snmp.beans.DataException: Error: OID not a leafnode.                                                            | The Error Message is thrown during set operation, if the OID selected is not a leaf node.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 12    | Error sending set request: com.adventnet.snmp.beans: DataException: Error: Creating Variable                                                              | If setting value for a columnnode of a table does not have rowstatus.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 13    | LineGraphBean Error: cannot plot string value Root.....                                                                                                   | The exception is thrown when plotting Graph for a leafNode, <ul style="list-style-type: none"> <li>1. If value of OID selected is not of Integer/TimeTicks/ type.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 14    | LineGraphBean Error: cannot plot these values .1.3..6.1.2.1.....: value .....: value .....: value                                                         | While plotting Line/Bar Graph, if the selected OID/LeafNode has syntax PhysAddress, NetworkAddress, IP Address, OBJECT IDENTIFIER.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 15    | Error: com.adventnet.snmp.beans.DataException: InvalidTable OID:(oid chosen)                                                                              | SnmpTable is started with OID which is not a Table OID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| S.No. | Error Message                                                                                                                                                                   | When it is displayed                                                                                                                                |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 16    | ErrorSendingPDU: Failed to Authenticate the Security Parameters, for user SnmpEngineEntry not found for address( hostname) port(portNo.)                                        | The exception is thrown while creating SnmpTable,<br>1. If the host name specified, is of different version than v3 which is set in settings table. |
| 17    | LineGraphBeanError: cannot plot string value xyz.                                                                                                                               | If the OID/LeafNode chosen for plotting Graph is of String Type.                                                                                    |
| 18    | Discovery failed for address (hostname) port (portno.)                                                                                                                          | If wrong port number is set in the MibSettings panel.                                                                                               |
| 19    | Time Sync Failed for user (user name)                                                                                                                                           | If wrong username/user password/priv password/ TargetHost/SecurityLevel is set in the MibSettings panel                                             |
| 20    | Error in Getting DataBase Connection:Please check the jdbc parameters: com.adventnet.snmp.beans.MibException: java.lang.ClassNotFoundException:                                 | If DriverName/URL/User Name/Password has been set wrong when loading MIBs from database                                                             |
| 21    | Error in Getting DataBase Connection:Please check the jdbc parameters: java.lang.ClassNotFoundException: (DriverName set)                                                       | If the mysql.jar class is not present in the classes directory.                                                                                     |
| 22    | Please enter the UserName                                                                                                                                                       | If the Username is not set for the v3 User.                                                                                                         |
| 23    | Sent request to hostName:port no.<br>Request Failed :SNMPv3 Error in Response.<br>usmStatsUnknownUserNames(.1.3.6.1.2.1.1...) Counter value = 2HostName                         | If Security parameters are set after setting the version v3 for a v1/v2 agent and request is made.                                                  |
| 24    | Enter the FileName of MibModule                                                                                                                                                 | While loading the MIBs file if OK button is clicked without selecting any file in "LoadMibDialog".                                                  |
| 25    | Error Loading MIB:(filename)<br>java.io.FileNotFoundException: Couldn't open stream for filename.cmi                                                                            | If any file chosen from outside the MIBs directory.                                                                                                 |
| 26    | Error Loading MIB:(filename with full path from home dir).cds<br>com.adventnet.snmp.mibs.MibException:The .cds file could not be loaded.                                        | When a .cds file is loaded.                                                                                                                         |
| 27    | Error Sending PDU: Failed to Authenticate the Security Parameters for user authUser USMUserEntry not found for this user. TimeSynchronizationFailure could have occurred.       | If ContextName/ContextEngineID is not set before making query for SnmpTable.(Database Mode)                                                         |
| 28    | Error in (get/getNext/getBulk)request to hostName:port no.<br>Failed to Authenticate the Security Parameters for user authUser USMUserEntry not found for Address hostname: 161 | If ContextName/ContextEngineID is not set before making get/getNext/getBulk request                                                                 |
| 29    | Error in get request from < hostname >: 161<br>Unable to encode PDU.                                                                                                            | get Request for a v3 User(Database mode)<br>AuthProtocol: MD5<br>Context Name,<br>ContextEngineID are not specified.                                |

| S.No. | Error Message                                                                                                                                                                                                                        | When it is displayed                                                                                                                                                                                                      |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                                                                                                                                                                                      | Same exception is thrown for getnext, getbulk and set operation also.(for AuthProtocol MD5&SHA)                                                                                                                           |
| 30    | Error in get request from < hostname >: 161<br>Failed to authenticate the security parameters for user privuser authKey length has to be 20.                                                                                         | get Request for a v3 User(Database mode)<br>AuthProtocol: SHA<br>Context Name,<br>ContextEngineID are not specified.                                                                                                      |
| 31    | can not plot the chosen variable:<br>iso.org.dod.internet.mgmt.mib2.interfaces.ifTable                                                                                                                                               | If IfTable OID is chosen for plotting Graph.<br>The Error will be thrown if the OID chosen is not a leaf OID.                                                                                                             |
| 32    | sent get request to tonyjpaul:161<br>Request Failed: SNMPv3 Error in Response: usm Stats Not InTimeWindows(.1.3.6.1.6.3.1.5.1.1.2.0) CounterValue =13 tonyjpaul                                                                      | During getRequest for a v3 user<br>Context Name,<br>ContextEngineID not specified.<br>Same Error Message is Thrown for other operations like getNext, getBulk, set                                                        |
| 33    | sent getbulk request to localhost:161<br>Request Failed: Get Response PDU received from 127.0.0.1.<br>Error Indication in response : This is a end of MIB View.<br>ObjectID: .1.3.6.1.2.1.1.9.1.4.9<br>NULLOBJECT:NULL               | If getBulk Operation is done for "org".(setting version v2/v3 for a v1 host)<br>if the OID/LeafNode selected is the last node of the mib.<br>The same Exception will be thrown for operations like getNext, getBulk also. |
| 34    | Error Sending set Request:<br>com.adventnet.snmp.beans.DataException: Error: Mib node unavailable for OID.                                                                                                                           | Setting value for an OID which is not having any leafnode.<br>Now it's thrown if we are choosing any OID from "enterprises".                                                                                              |
| 35    | sent get request to < hostname >:161<br>Request Failed: Get Response PDU received from 192.168.1.182<br>Error Indication in response : There is no such instance in this MIB.<br>ObjectID: .1.3.6.1.2.1.1.9.1.4.9<br>NULLOBJECT:NULL | Get Operation on sysServices node for a v3 agent.<br>This Error is thrown if the leafnode sysServices is not implemented by the agent.                                                                                    |
| 36    | sent get request to <hostname>:161<br>Request Failed: Get Response PDU received from 192.168.1.182<br>Error Indication in response : A no creation error occurred.<br>Errindex:1                                                     | During set operation on ipRouteDest which has read-write access & syntax of datatype:IP Address for a v3 user.<br>As values cannot be set if the column is not of Row-Status type.                                        |
| 37    | sent get request to <hostname>:161<br>No data available in this subtree                                                                                                                                                              | When doing a get request for a v2 agent at OID "transmission"(.1.3.6.1.2.1.10) Exception is thrown when no data is available for that particular instance of OID.                                                         |

| S.No. | Error Message                                                                                                                                                                                                                                                      | When it is displayed                                                                                               |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 38    | Error in getting Database Connection . Please check the jdbc Parameters:<br>com.adventnet.snmp.mibs.MibException: java.sql.SQLException: No suitable Driver.                                                                                                       | Error is thrown when connecting to the database for an agent of any version, if the DriverName set is not correct. |
| 39    | Error in Getting DataBase Connection:Please check the jdbc Parameters: java.sql.SQLException: No suitable Driver.                                                                                                                                                  | This error is thrown when the URL set is not a valid URL for connecting to database.(mysql->msql)                  |
| 40    | Error in Getting DataBase Connection:Please check the jdbc Parameters: java.sql.SQLException: Cannot connect to MYSQL sever on smplinux:3306. Is there a mysql server is running in the machine/port you are trying to connect to? (java.net.UnknownHostException) | This error is thrown when the URL set is not a valid URL for connecting to database.(snmplinux->smplinux)          |
| 41    | Error in Getting DataBase Connection:Please check the jdbc Parameters: java.sql.SQLException: General error: Unknown database "<tst>"                                                                                                                              | This error is thrown when the URL set is not a valid URL for connecting to database.(test->tst)                    |
| 42    | sent set request to <hostname>:161<br>Request Failed: SNMPv3 Error in Response : usmStatsNotInTimeWindows(.1.3.6.1.6.3.15.1.1.2.0)Counter value = 75 <hostname>                                                                                                    | Error thrown if the request is made after a certain interval of time..                                             |
| 43    | sent get request to <hostname>:161<br>Request Failed: Get Response PDU received from 192.168.1.182<br>Error Indication in response : There is no such object in this MIB.<br>ObjectID: .1.3.6.1.2.1.8.1.0<br>NULLOBJECT:NULL                                       | This OID is not instrumented for the agent you are querying for or no data is available in this OID.               |

## 6.15.1.11 Customization

The MibBrowser application that is bundled with AdventNet SNMP API is developed using the MibBrowser bean. Developers can customize the MibBrowser application to their own needs. This section explains the steps involved in customizing the MibBrowser application.

Customization of the MibBrowser application is explained in reference to the MibBrowserApplication file available in the <MibBrowser> directory.

1. The title of the MibBrowser application can be customized. By default, the title is "AdventNet MibBrowser".

```
public MibBrowserApplication()
{
    super("AdventNet MibBrowser");
```

The title can be set to the window because the MibBrowser bean is a panel. The above title can be changed to the user's choice.

2. You can set some of the values, such as remote host, MIB filename, etc. to be initialized when the application is started. The application can be customized to get the properties from the command line or from the application itself. The following are some of the properties that can be set.
  - remote host - mibrowser.setTargetHost();
  - remote port - mibrowser.setTargetPort();
  - community - mibrowser.setCommunity();
  - SNMP version - mibrowser.setSnmpVersion();

Here, mibrowser is the instance of the MibBrowser bean.

3. You can customize the display of the MibBrowser menu bar. By default, it is set to false. You can display the menu bar by setting ***mrowser.setMenuBarVisible()*** to true.
4. You can customize the display of the MibBrowser display area. By default, the Result area and the MibDescription area are shown. You can set the MibBrowser display view to show the MibDescription panel, the ResultDisplay panel, or the MultiVarbind panel using the method ***setMibBrowserDisplayView(int view)***.
5. You can add and remove toolbar buttons from the MibBrowser. The instance com.adventnet.snmp.uiToolBar can be obtained from the method ***getToolBar()***.

```
ToolBar toolbar = mrowser.getToolBar();
//Exit button is added as below and ActionListener is implemented.
JButton button = toolbar.addButton("Exit",
new ImageIcon(getClass().getResource("exit.jpg")), "Exit
MibBrowser");
button.addActionListener(this);

//Removing button from the Toolbar using index. Even the separator
//is a component and once the component is removed the index will
//be adjusted. Please be careful.
toolbar.removeComponentAt(int i);
```

6. You can also add or remove menu item from the MibBrowser menu bar.

```
//Exit MenuItem is added as below and ActionListener is implemented.
JMenuBar bar = mrowser.getMenuBar();
JMenu fileMenu = bar.getMenu(0);
```

```
fileMenu.addSeparator();
fileMenu.add(exitItem = new JMenuItem("Exit", 'x'));
exitItem.addActionListener(this);
```

7. The Help and the About image can also be customized. The default help file has to be help/index.html file from the installed directory. The "about" dialog box image can be replaced by changing the about.jpg image file available in the <AdventNet/SNMPAPI/images> directory.

## 6.15.1.12 FAQs

1. How do I give Hex strings for SET values in MibBrowser?
2. How do I give Hex values in the ContextEngineID or in the ContextName text fields?
3. What are the units for timeout and retry values?
4. How do I set values for the table variables?
5. If I load the MibBrowser applet, I get the error "Error Sending PDUSecurity Exception connecting to remote host" in the browser. Why is this so?
6. I do not get the "NO HOST Specified" error. What should I do?
7. How can I load multiple MIB files in MibBrowser?
8. When I ask for 10 rows in an SNMP table, the GETBULK returns only 6 rows and the last attribute of the sixth row is null. The sixth row seems to be truncated. What should I do?
9. I use JDK 1.2. How do I invoke MibBrowser as an applet through applet viewer?

### **1. How do I give Hex strings for SET values in MibBrowser?**

The SnmpString class accepts Hex strings in a certain format. Any string that starts and ends with a single quote(') is interpreted as an Hex string. The individual bytes should be separated using a colon(:). For example, if you need to enter 0x2a304cab, it should be supplied as '2a:30:4c:ab'.

### **2. How do I give Hex values in the ContextEngineID or in the ContextName text fields?**

The Hex values should start with a 0x or 0X. Therefore, if you set a value for contextID or contextName, it should be 0xHHHHHH.

### **3. What are the units for timeout and retry values?**

Both the timeout and retry values should be given in seconds. If you give the timeout value in milliseconds, it takes much time to get timed out. For example, a value of 1000 waits for 1000 seconds.

### **4. How do I set values for the table variables?**

To create a new row in a table:

1. Define a column with SYNTAX RowStatus, and the definition for the table should have RowStatus object defined.
2. Select the Table node from the tree and the Table button from the toolbar to display the corresponding table.
3. Right-click on the table header where the name of the column is displayed. It displays a menu with the following options:
  - View Graph for Selected Rows
  - Add a New Row to the Table
  - Delete the Selected Rows from the Table
4. Select Add a New Row to the Table. It displays a window for entering the values of the table.
5. The value for the column with RowStatus syntax should be 4 for creating a new row.
6. Click OK after entering all the values.

If RowStatus is not present in the table definition, you can only modify the existing row by double-clicking the corresponding cell in the table.

**5. If I load the MibBrowser applet, I get the error "Error Sending PDUSecurity Exception connecting to remote host" in the browser. Why is this so?**

Applets are not allowed to talk to any host apart from the Web server from which they were downloaded. Make sure that SAS is also running along with the Web server.

**6. I do not get the "NO HOST Specified" error. What should I do?**

Before making any request, the host name or the IP address of the machine in which the agent is running should be specified in the "Host" text field of MibBrowser.

**7. How can I load multiple MIB files in MibBrowser?**

To load multiple MIBs, files should be separated by a blank space and be given within double quotes. For example,

*java MibBrowserApplication -m "mibs/RFC1213-MIB mibs/RFC1271-MIB mibs/RFC1155-MIB" -h localhost -c public.*

If you use MibBrowser.sh, edit the file accordingly.

**8. When I ask for 10 rows in an SNMP table, the GETBULK returns only 6 rows and the last attribute of the sixth row is null. The sixth row seems to be truncated. What should I do?**

The number of rows you get back may be limited by the PDU size permitted by your agent, manager, or transport.

**9. I use JDK 1.2. How do I invoke MibBrowser as an applet through applet viewer?**

From JDK1.1, the appletviewer no longer takes the CLASSPATH setting into consideration. Therefore for the applets, the following command is to be given.

```
appletviewer -J-Xbootclasspath:..;
..\.\\jars\\AdventNetSnmp.jar;..\\.\\jars\\AdventNetLogging.jar;
..\\.\\sasapps.jar; c:\\jdk1.2\\jre\\lib\\rt.jar
```

To load from the browsers, the HTML file should also be changed accordingly.

Applets could instead be packaged into jar files for easy use. Also, with JDK1.2, you can specify dependencies on other jars through extensions. Therefore, if you create an applet that uses AdventNet Beans and the target platform is the JDK1.2-plug-in, you need to include the CLASSPATH.

## 6.15.2 TL1 Craft Interface

**TL1 Craft Interface** is an user-friendly GUI tool that enables craft operators to easily manage the TL1 infrastructure. It helps lab technicians and field engineers to test, monitor, administer, and provision multiple TL1 agents. While the normal Telnet interface is too simple, this tool offers a sophisticated and productive environment.

This section explains the functionality available in the graphical interface and ways to interact with TL1 agents. The TL1 Craft Interface tool is built over AdventNet TL1 API and can manage TL1 devices from multiple equipment vendors.

### Key Features

Following are the key features offered by the TL1 Craft Interface:

- **Connectivity with multiple TL1 devices** : Easily manage and monitor multiple TL1 devices simultaneously.
- **Load pre-built TL1 commands** : This will simplify the tedious task of dealing with various device-specific TL1 messages.
- **Load pre-built message templates** : Helps administrators to easily provision/configure a particular element in an NE such as, Equipment, Facility, Cross-connect etc. The message templates are XML-based definitions (Command Set) and are built using TL1 Message Builder.
- **Automatic Message Rationalization** : Allows craft operators to easily understand messages received from multiple TL1 devices. This is done by upgrading the received messages based on the TL1 message definitions.
- **Bulk Message Support** : Allows field engineers to run routine diagnostic tests. These tests can be carried out on-demand to isolate problems on a particular element within an NE.
- **Multiple Transport Protocols** : Allows craft operators to communicate with TL1 devices via, TCP, Telnet, or Serial transport. The tool also provides support for plug-in custom transport protocols.
- **Session Logging** : Allows administrators to generate and browse historic information of TL1 devices. Offers transaction-based logging as well as raw data logging.
- **Re-brandable User Interface** : Allows vendors to exhaustively customize and bundle this tool as part of their management application. This tool also supports **internationalization** which allows vendors to customize this tool to suit their country and language.

### What This Section Explains

---

- Getting Started
  - Working with TL1 Craft Interface
  - Files Used by TL1 Craft Interface
  - How to Configure TL1 Craft Interface?
  - Internationalization
  - Re-branding TL1 Craft Interface
-

## 6.15.2.1 Getting Started

- Main Screen
- Actions
- Loading Files
- General Options

### Main Screen

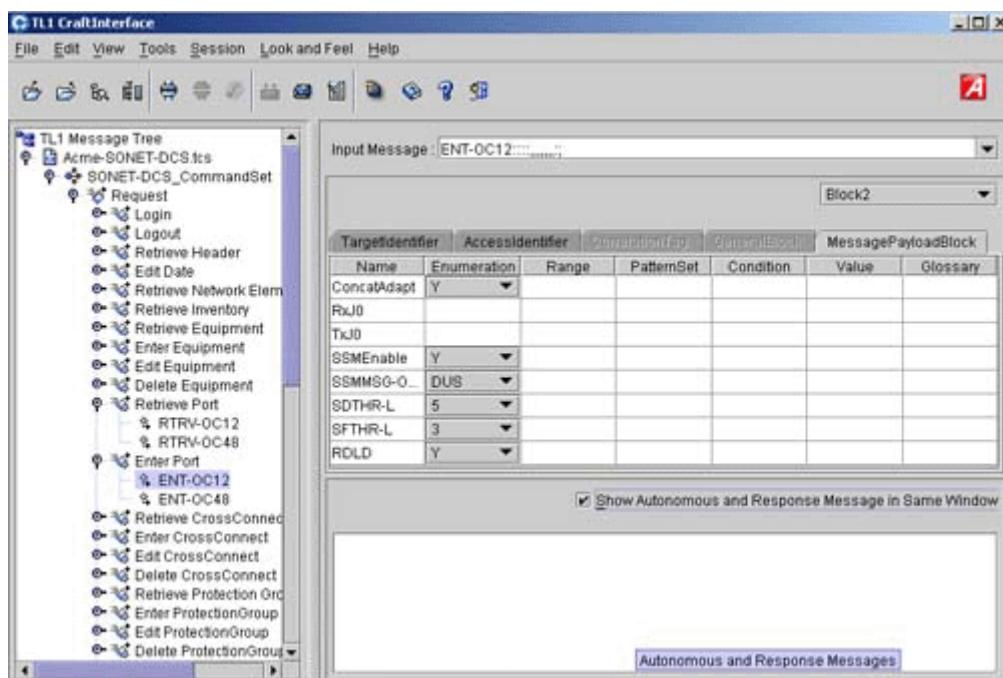
The main screen of the TL1 Craft Interface consists of two panels:

- **Left Panel**
- **Right Panel**

The Left Panel holds the Message Tree and is used for loading TL1 commands. Multiple files can be loaded to the Message Tree. The commands loaded in the tree can be selected and sent to the device directly. The Message Tree allows you to load command set, data set, and text files.

The Right Panel is split into two parts. The upper half holds the Input Message details. It contains a text field to show details about the selected TL1 Input Message. It also holds a table that individually displays the parameters specified in each block in the TL1 command. Select a particular block to view the parameters defined in the block. You can also edit the parameters under each block, which gets reflected in the Input Message field.

The lower half holds the text area which display messages received from the TL1 device. This text area can be combined or split. In the combined fashion, all the messages are received in the single text area. In split fashion, responses and notifications are received separately. You can change the mode using the **Show Autonomous and Response Message in Same Window** Check box.



## Actions

### Toolbar Options

Following are the actions that can be performed from the toolbar in the TL1 Craft Interface.

|                                                                                     |                                                          |
|-------------------------------------------------------------------------------------|----------------------------------------------------------|
|    | Load command set, data set, or text files.               |
|    | Unload command set, data set, or text file.              |
|    | Find a particular node in the TL1 Message Tree.          |
|    | Shift the mode from tree to list.                        |
|    | Shift the mode from list to tree.                        |
|    | Open a connection with the TL1 device.                   |
|    | Close the connection with the TL1 device.                |
|    | View the TL1 session properties.                         |
|    | Send messages to the TL1 device.                         |
|    | Switch to Bulk mode to send multiple messages at a time. |
|    | Switch to Normal mode to send one message at a time.     |
|    | View default settings of the TL1 Craft Interface.        |
|   | Clear messages from the text area.                       |
|  | Open Help Documentation in a Web Browser.                |
|  | Show Context-sensitive help of a selected component.     |
|  | Close Craft Interface Application.                       |

### Shortcut Keys

Following are the shortcut keys to perform various actions available in the TL1 Craft Interface.

| Shortcut Key | Action                                         |
|--------------|------------------------------------------------|
| Ctrl+Alt+C   | Load a Command Set file in the Message Tree    |
| Ctrl+Alt+D   | Load a Data Set file in the Message Tree       |
| Ctrl+Alt+T   | Load a Text file to the List                   |
| Ctrl+U       | Unload files from the Message Tree or List     |
| Ctrl+F       | Find a particular node in the TL1 Message Tree |
| Ctrl+O       | Open connection with the TL1 device            |
| Ctrl+W       | Close the TL1 connection                       |
| Ctrl+M       | Send messages to the TL1 device                |
| Ctrl+Alt+B   | Switch to Bulk Mode                            |
| F3           | Move to Tree/List mode                         |
| F4           | Open Session Properties window                 |
| F9           | Open Log Message Viewer window                 |
| Alt+F4       | Closes the Craft Interface tool                |
| F1           | Opens Help Documentation in a Web browser.     |

### Loading Files

TL1 Craft Interface enables loading of pre-built TL1 commands and simplifies the tedious task of dealing with various device-specific TL1 messages. Multiple files can be loaded to the TL1 Message Tree and can be selected to be sent to the device. You can load command set, data set, or text files in the TL1 Message Tree. These files can be created using the Message Builder tool.

This section explains how to load and unload files from the Craft Interface.

### To Load a File

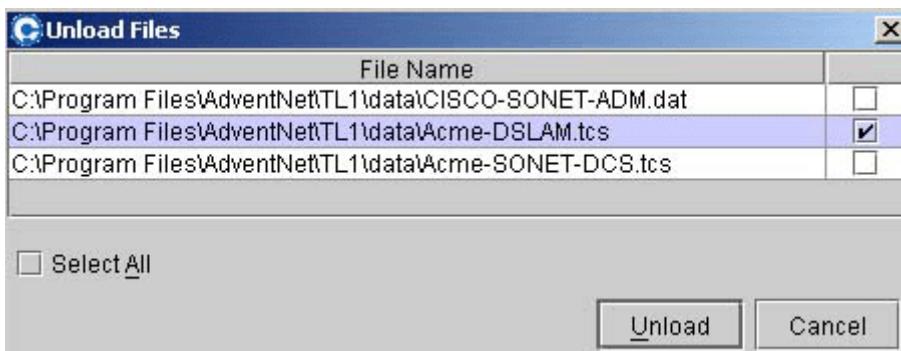
1. Click the **Load** button from the File menu. Select the file type, i.e. **Command Set**, **Data Set**, or **Text**.
2. A Load dialog opens up. Select the file to load.
3. Click the **Load** button to load the file in the TL1 Message Tree.
4. Click the **Cancel** button to cancel the load operation.



**Note:** If you would like to load command set and data set files, you must first move to the tree mode. To load text files, you must move to the list mode.

### To Unload a File

1. Click the **Unload** button from the File menu or toolbar. This opens up a Unload dialog that lists all the loaded files.
2. Select the file you wish to unload and click the **Unload** button.
3. Use the **Select All** check box to unload all the loaded files.
4. Click the **Cancel** button to cancel the operation.



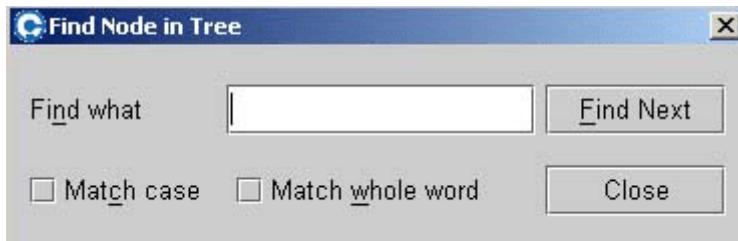
## General Options

Following are some of the general options available in the TL1 Craft Interface.

- Find option
- Look and Feel
- Generalize and Categorize option
- Expand and Collapse option
- Glossary View in Command Set
- Show Messages in the same window
- Clear Messages
- Conversion Tool
- Context-sensitive Help

### Find Option

This option is invoked by selecting **Find** from the Edit menu or from the toolbar. It searches a particular child node under a selected node in the TL1 Message Tree easily.



| Option           | Description                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Find What        | Uses this text in the search.                                                                                                                                 |
| Find Next        | Searches for the next text in the TL1 Message Tree.                                                                                                           |
| Close            | Ends the search operation and closes the dialog.                                                                                                              |
| Match case       | Searches for case-sensitive occurrences of a text. This limits the search and locates the text that matches the uppercase and lowercase characters you enter. |
| Match whole word | Search for occurrences of a text as whole words.                                                                                                              |



**Note:** The find option is supported only in the Tree mode.

## Look and Feel

This option changes the look and feel of the Craft Interface. Three options are available, **Metal**, **Motif**, and **Native**. Any one of these options can be selected based on the platform. This menu can be hidden from the menu bar by disabling it in the **Tools -> Options Window**. The default UI Look and Feel used by the tool is Metal.

## Generalize and Categorize Message Tree

This option is used to display the commands in the Message Tree either command-based or category-based. By default, all messages are listed command wise. To display the commands category wise, right-click on the Request node and select the **Categorize** button. Select the **Generalize** button to display them command-wise.

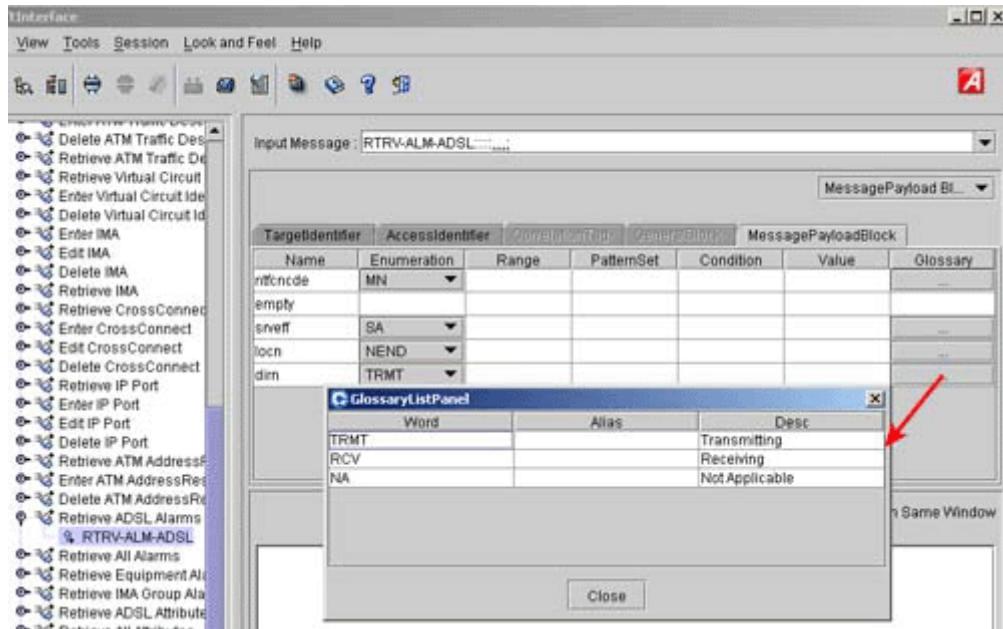
## Expand and Collapse Option

This option is used to expand and collapse all the nodes in the TL1 Message Tree. To perform this function, select the option by doing a right-click on the root node of TL1 Message Tree.

## Glossary View in Command Set

Glossary option in Command Set allows you to view description of a parameter, enumeration or range values. To use the glossary option, there must be an entry in the word list of that command set file. Also this entry must be associated with the parameter.

Assuming there is word list entry in the glossary for a set of parameters. Now, load the command set file and select the node in the command set which has a word list defined. The right panel displays a table as shown below. Click the "..." button present in the glossary column. The Glossary List panel appears which contains description about that parameter.



## Show Messages in the Same Window

This option allows both Autonomous and Response messages to be shown in the same window. You can enable it by selecting it from the right-side panel of the main frame. By default, there will be two text areas; one for showing the response and acknowledgment messages and the other for showing autonomous messages. Selecting this option allows all the messages to be displayed in the same text area.

## Clear Messages

This option can be used to clear all the messages displayed in the text area. It can be selected by clicking the **Clear Text** from the Edit menu. You can also clear the messages through the text area pop up menu.

## Conversion Tool

This tool is used to convert the input commands specified in the data set (.dat) file to a textual form. The resultant text file will have the complete list of input commands which can be loaded in Craft Interface as a list. This tool can be opened by selecting the **Data To Text Conversion** button from the Tools menu.

## Context-sensitive Help

This option is used to describe the functionality of a particular component in the Craft Interface. To use this option, select the context-sensitive button available in that dialog and place it on the component you wish to know.

## 6.15.2.2 Working with TL1 Craft Interface

---

- How to Establish a Connection?
  - How to Manage Multiple Connections?
  - How to Send and Receive TL1 Messages?
  - How to Send and Receive Bulk Messages?
  - How to View Log Messages?
-

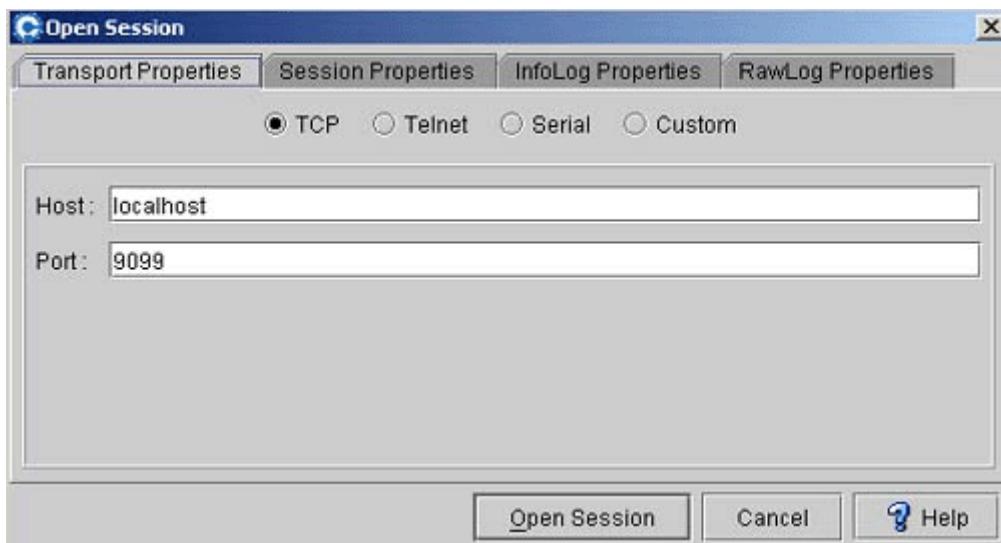
## 6.15.2.2.1 How to Establish a Connection with the TL1 Device?

- 
- Overview
  - Transport Properties
    - TCP
    - Telnet
    - Serial
    - Plugging your own Transport Protocol
  - Session Properties
  - Log Properties
  - How to Terminate the Connection
- 

### Overview

Establishing a connection with a TL1 device is the first step to manage any TL1 device. Once a connection is successfully established, you can send messages to the device and get responses. The TL1 Craft Interface is designed to handle multiple device connections at the same time. This is done by means of a Session Manager which manages all the TL1 connections. The tool is built over common Transport Provider Framework and supports multiple transport protocols such as **TCP**, **Telnet**, and **Serial**. You can also plug in your own transport protocol in the Craft Interface and send TL1 messages.

To establish a connection with the TL1 device, click the **Open Session** button from the Session menu or from the toolbar. The **Open Session** dialog is displayed as shown in the figure. Select the transport protocol such as **TCP**, **Telnet**, or **Serial** to communicate with the TL1 device and specify the connection properties. For example, you must specify the host and port in the case of **TCP**.



## Transport Properties

By default, the TL1 Craft Interface supports transport protocols such as TCP, Telnet, and Serial. But you can also plug in your own transport protocol in the craft interface to work with. The transport-related options specific to each protocol is discussed here.

### a) TCP

In this case, you need to specify two mandatory parameters, Host and Port of the TL1 device where the agent is running. The default values for these parameters are given in the table.

| Parameters  | Default Value |
|-------------|---------------|
| Host Name   | localhost     |
| Port Number | 9099          |

### b) Telnet

In the case of Telnet, there are various options such as Host, Port, Command Prompt, Login Prompt, User Name, Password Prompt, Password, and Time out. The mandatory parameters are Host, Port, and Command prompt. The default values for these parameters are given in the table.

| Parameters      | Default Value |
|-----------------|---------------|
| Host Name       | Null          |
| Port            | 23            |
| Command Prompt  | \$            |
| Login Prompt    | login:        |
| User Name       | Null          |
| Password Prompt | Password:     |
| Password        | Null          |
| Login Timeout   | 5000          |

### c) Serial

In the case of Serial (RS232), the options are Port, Baud rate, Flow control, Data bits, Stop bits, and Parity. These parameters should be properly specified based on the settings configured on the TL1 device. The default values for these parameters are given in the table.

| Parameters   | Default Value |
|--------------|---------------|
| Port         | COM1          |
| Baud Rate    | 9600          |
| Flow Control | None          |
| Stop bits    | 1             |
| Data bits    | 8             |
| Parity       | None          |

### d) Plugging your own Transport Protocol

Apart from the Transport Protocols supported, users can plug in their own transport protocol. Follow the steps given below to add your transport protocol for TL1 communication.

1. Write your own transport protocol implementation that implements the **TL1TransportProvider** interface and set it in the CLASSPATH.

2. Select the user-defined option and type the full class path of your protocol implementation in the Transport Provider field. In the case of **TCP**, it is **com.adventnet.tl1.transport.tcp.TcpTransportImpl**.
3. Add all connection-related properties required for the transport protocol in the table. You can refer the default protocol implementations available in the *<Web NMS Home>/default\_impl* directory.
4. Select the mode of communication. It can be either **Normal** or **Craft**.
5. Click the **Open Session** button to open a connection using the specified transport protocol.

## Session Properties

The table below lists the common options which can be used across all the transport protocols.

| Parameters                          | Description                                                                                                                                                                                                                                                                                             |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mode</b>                         | This can be either <b>Normal</b> or <b>Craft</b> . In Normal mode, messages are buffered in a queue, then parsed and sent to the application. In Craft mode, messages are given to the application directly without any processing on the session.                                                      |
| <b>Connection Handler</b>           | Represents the interface <b>ConnectionHandler</b> . Users can do some special tasks while opening and closing the connection (such as login and logout).                                                                                                                                                |
| <b>Message Parser</b>               | Represents the interface <b>TL1Parser</b> . This interface parses the TL1 messages and generate message objects. By default, <b>com.adventnet.tl1.parser.TL1MessageParser</b> is implemented. You can also plug in your own parser implementation.                                                      |
| <b>Message Formatter</b>            | Represents the interface <b>MessageFormatter</b> . This interface allows you to filter or format specific TL1 messages at runtime. Users can plug-in their own filter / formatter by implementing this interface. By default, it is <b>null</b> .                                                       |
| <b>Message Rationalizer</b>         | Represents the interface <b>MessageRationalizer</b> . This interface allows you to upgrade messages based on the XML message definitions (command set) or filter specific TL1 messages. Users can plug in their own rationalizer by implementing this interface. By default, its value is <b>null</b> . |
| <b>Partial Message Accumulation</b> | Option to provide or accumulate partial messages received from the device. If set to true, all partial messages are accumulated and given only after receiving a response with proper terminator (;).                                                                                                   |
| <b>Prefix and Suffix</b>            | Append special strings at the start and end of each TL1 message. This is optional and may not be applicable for all devices. The default prefix is <b>\r</b> and the suffix is <b>null</b> .                                                                                                            |

## Log Properties

The Log Properties is split into Raw Log and Information Log.

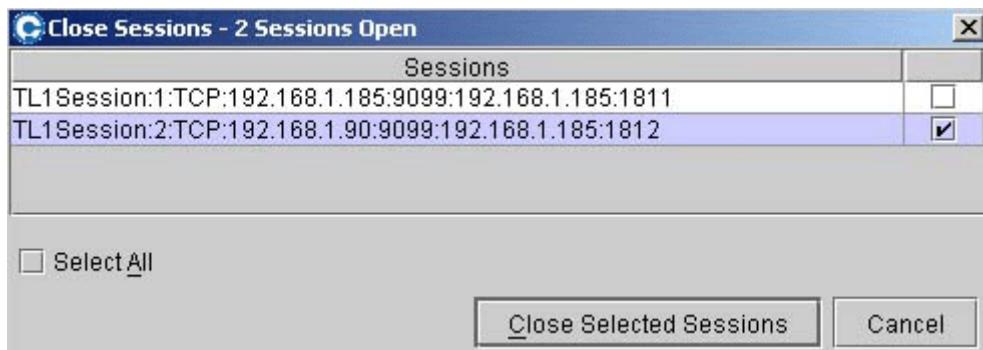
| Parameters       | Description                                                                                                                                                                                                                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>File Name</b> | Represents the name of log file.                                                                                                                                                                                                                                                                                                                                     |
| <b>Pattern</b>   | Pattern indicates the order in which the log file name should exist.<br><br>%n represents the log file name.<br>%d represents the date at which the log file is generated.<br>%t represents the time at which the log file is generated.<br>%c represents the log file count generated for that particular connection.<br>The date and time are optional in pattern. |

| Parameters               | Description                                                                                                                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Timestamp</b>         | Option to set the Timestamp in each log message. The time will be given in hh-mm-ss format.                                                                                                   |
| <b>Append File</b>       | Appends the log information to the same log file that was previously used by this connection.                                                                                                 |
| <b>Rollover Size</b>     | Maximum size of a log file after which a new log file will be created. The size should be given in bytes. You can give a value of 0 if you do not want log files to be created based on size. |
| <b>Rollover Count</b>    | Maximum log file count for a particular device connection.                                                                                                                                    |
| <b>Rollover Time</b>     | Time that must be specified after which a new log file will be created. The time should be given in the hh-mm-ss format.                                                                      |
| <b>Rollover Interval</b> | Interval that must be specified after which a new log file will be created. The interval should be given in milliseconds.                                                                     |

## How to Terminate the Connection

To close an established connection, follow the steps given below.

1. Select the **Close Session** button from the Session menu or through the toolbar. The Close dialog is displayed. This dialog displays all the established sessions.
2. Select the sessions you wish to close and click the **Close Selected Sessions** button.
3. Use the **Select All** check box to close all the established sessions.
4. Click the **Cancel** button to cancel the close operation.

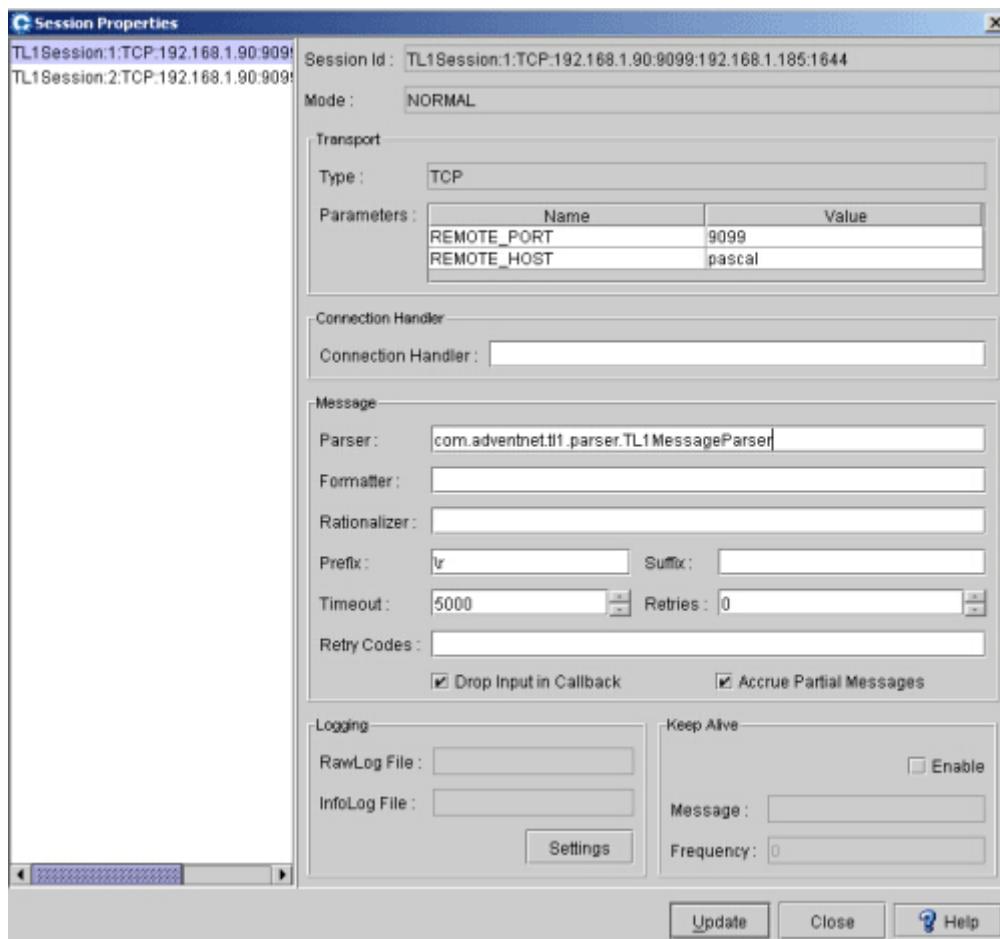


## 6.15.2.2.2 How to Manage Multiple Connections?

One unique feature in the TL1 Craft Interface is that, it can interact with multiple TL1 devices simultaneously. This helps field engineers to manage multiple TL1 devices at the same time. The Craft Interface connections are managed by the Session Manager. These connections and their associated parameters can be viewed through the Session Properties window. The Session Properties window can be invoked by selecting the **Properties** button from the Session menu or through the toolbar.

The User Interface of the Session Properties window is split into two panels. The left panel displays all the established sessions and the right panel is to show the properties pertaining to each connection. You can select a particular session and update their properties.

The image below shows the Session Properties window with default parameters.



**Note:** The Session Properties window can be viewed only if there is at least one established connection.

### 6.15.2.2.3 How to Send and Receive Messages?

After successfully establishing a connection with the TL1 device, you can query by sending commands. The commands can be sent from the Craft Interface in one of the following ways:

- Using List
- Using Command Set
- Using Data Set

#### Using List

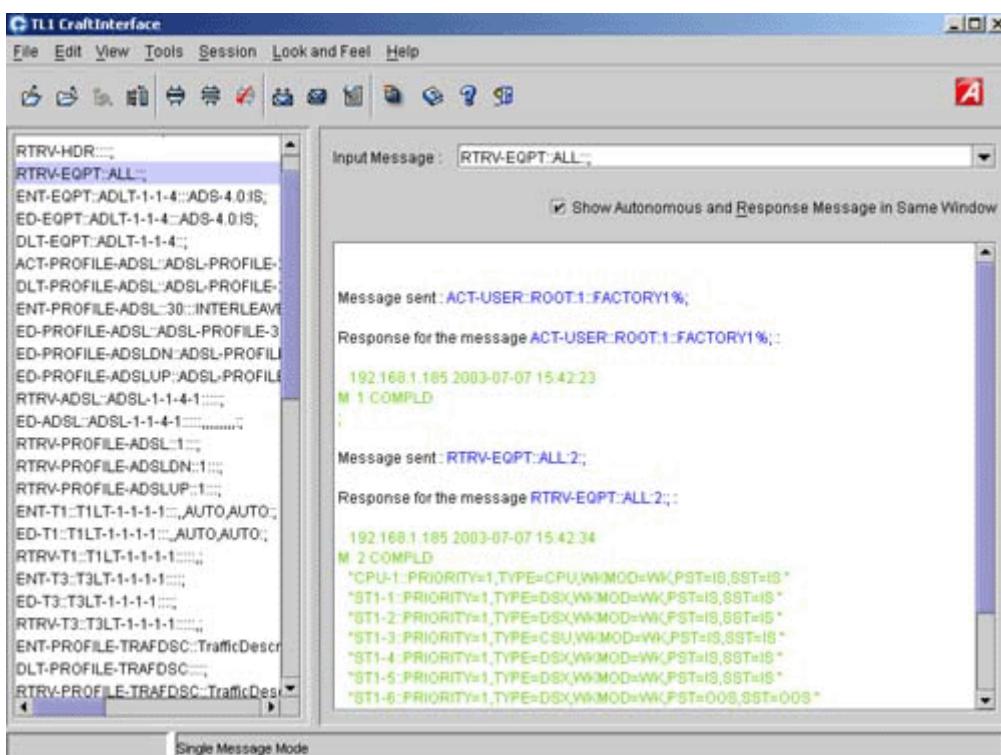
This is the crude and easy way of sending commands to the device and get responses. In the list mode, you can either type a command manually in the text field shown in the right panel or load commands from a text file. Click the **Send** button to send the commands. Alternatively, you can also double-click on the selected command in the list or use the **Enter** button to send the command. The responses will be displayed in the text area of the right panel.

In this mode, commands can be sent one at a time, or multiple commands can be selected to be sent as bulk. The figure below shows how to perform the query operation one at a time.

To send one command at a time:

1. Select the command from the list.
2. Edit the command (if you wish) in the right panel.
3. Click the **Send** button to send the command.

The responses can be viewed in the right panel.



The bulk mode of sending commands is discussed in the next section.

## Using Command Set

You can also send commands to the device by loading the command set file. Follow the steps mentioned here to send commands using the command set file:

1. Select the command from the message tree.
2. Edit the command (if you wish) in the right panel. The Craft Interface splits the command into parameter blocks and each block can be edited separately. If default values for the parameter is specified in the command set file, they are displayed in the combo box. You can simply select the value from the combo box or edit these values (if necessary) in the input message field.
3. Click the **Send** button to send the command. The responses can be viewed in the right panel.

## Using Data Set

The data set way of sending commands to the device is same as command set. The only difference is that, the message cannot be edited field. Follow the steps mentioned here to send commands from the data set:

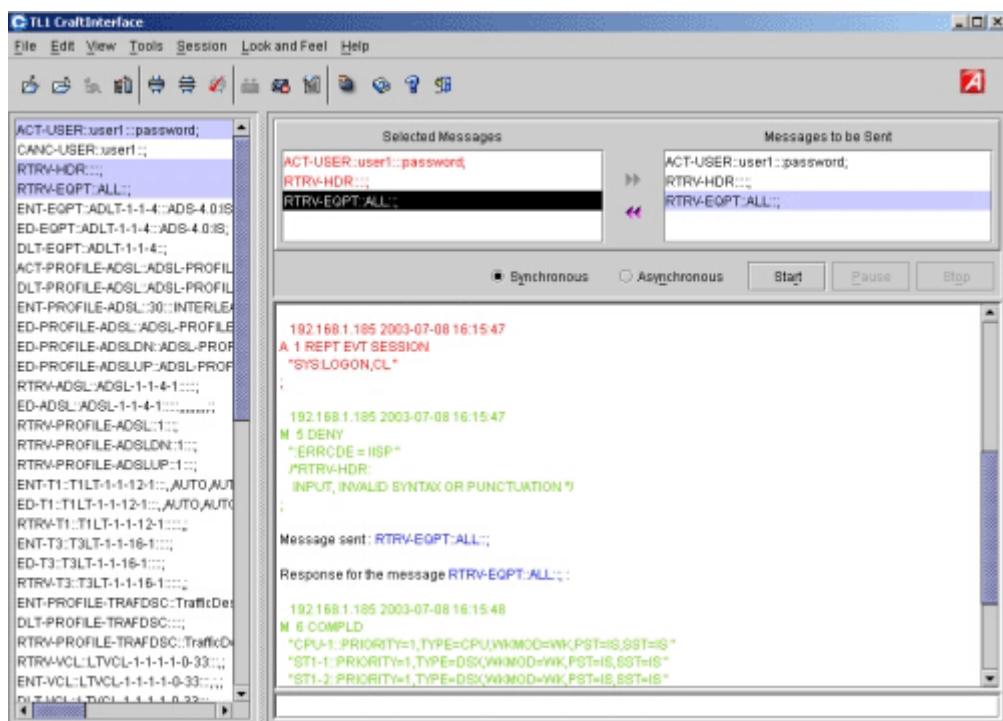
1. Select a input message data from the message tree.
2. Edit the command (if you wish) from the input message field in right panel.
3. Click the **Send** button to send the command. The responses can be viewed in the right panel.

## 6.15.2.2.4 How to Send and Receive Bulk Messages?

In TL1 Craft Interface, one or more messages can be selected to be sent at a time. This section explains how to perform this function from the Craft Interface. At present, the bulk mode is supported only in Data Set and Text file.

To send multiple commands at the same time:

1. Load a Data Set or Text file.
2. Select commands from the data set or list with **Ctrl** button pressed. All selected commands will be displayed in the right panel under **List of all Messages**.
3. Select the commands in the order they have to be sent and press the **>>** button. These commands will be put in the send list.
4. Use the **<<** button to remove selected commands from the send list.
5. Choose the mode of transmission (Synchronous/Asynchronous).
6. Click the **Start** button or **Send Bulk Messages** button to send the commands. The responses can be viewed in the right panel.
7. Use the **Pause** button to pause the send operation. You can click the **Resume** button to resume the operation again.
8. Use the **Stop** button to stop the send operation.



## 6.15.2.2.5 How to View Log Messages?

TL1 Craft Interface provides an option to view the log files generated for each device connection from the Log Message Viewer. The log files are created in two formats, **Information log** and **Raw log**. The information log contains textual description of each log record and the raw log contains the actual messages exchanged through the session. The Log Message Viewer has the facility to view the log files of each TL1 Session.

The Log Message Viewer can be invoked by selecting the **Logs** button from the Session menu. The User Interface of Log Message Viewer is split into two panels. The left panel has the list of sessions and the right panel contains the log message details.



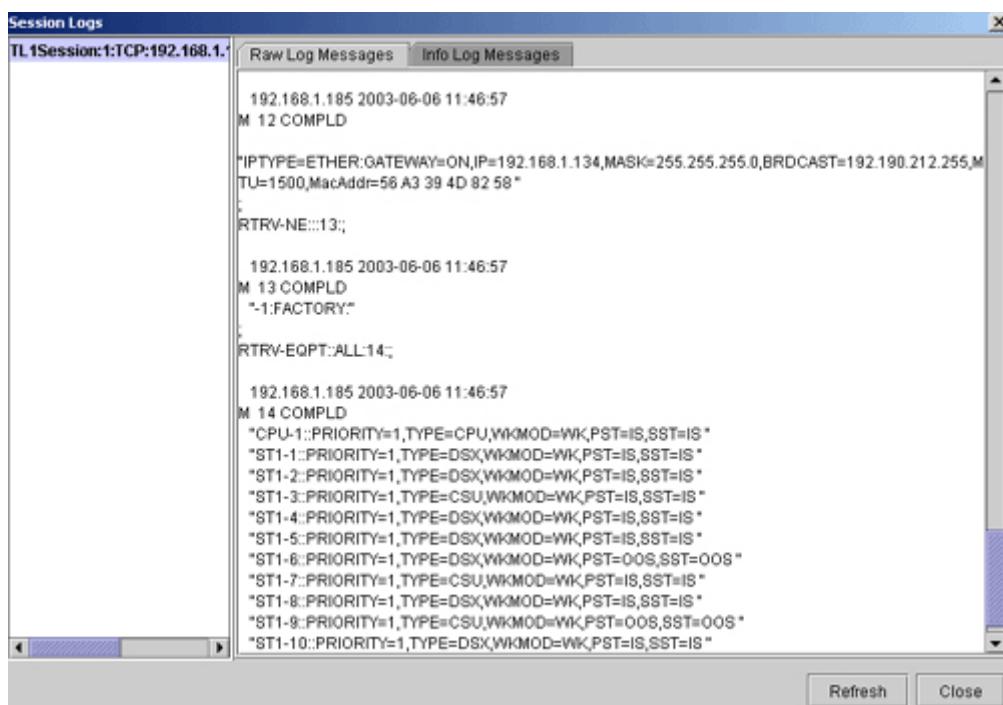
**Note:** The Log Message window can be viewed only if there is at least one established connection.

### Raw Log

To open a raw log,

- Select the session name from the left panel.
- Click the Raw Log Messages tab.

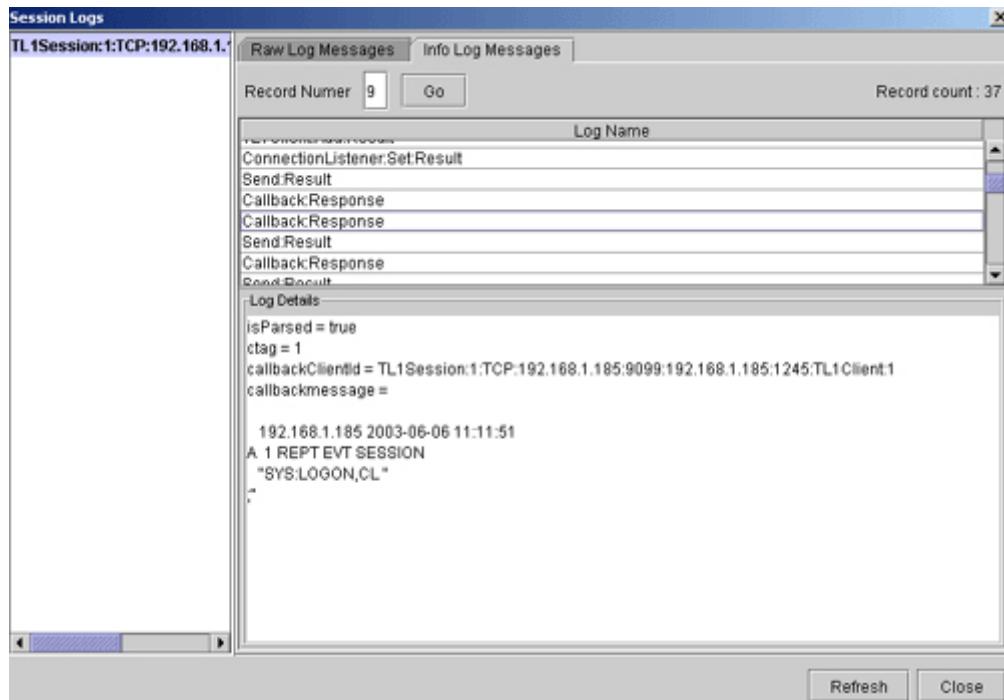
Now you can view all the messages exchanged through this session.



### Information Log

To open a information log,

- Select the session name from the left panel.
- Click the Information Log Messages tab. This panel contains a Log Name table.
- Select the Log Name and the details regarding each log record will be displayed in the Log details pane beneath the Log Name table.



**Note:** Although multiple log files are created for each individual connection based on the Rollover criteria, you can only view the log file that is currently in use.

## 6.15.2.3 Files Used by TL1 Craft Interface

Following files are used by the TL1 Craft Interface for performing various functions.

### 1) Command Set file (.tcs)

The Command Set file contains TL1 command definitions in XML format. Apart from command definitions, it also contains response message and autonomous message details specific to each TL1 device. You can use the **TL1 Message Builder** tool to create these message definitions. Please refer to TL1 Message Builder section for more details on the structure of the Command Set file.

### 2) Data Set file (.dat)

The Data Set file contains values for each command defined in the Command Set in XML format. You can use the **TL1 Message Builder** tool to create data set values. Please refer to the TL1 Message Builder section for more details on the structure of the Data Set file.

### 3) Text file (.txt)

The text file contains a list of input messages which can be loaded in the list. The input messages must be defined in separate lines. You can also use the conversion tool to convert the existing data set files to a text file.

### 4) Configuration file (tl1craftinterface.config)

The configuration file is used to store the default settings of the Craft Interface. You can use the **Options Window** in the Craft Interface to modify the default settings. The default settings include Session, Message, GUI, and Log options. Please refer to the Configuring the TL1 Craft Interface section for more details.

### 5) Properties file (tl1craftinterface\_i18n.properties)

This file can be used as a reference for creating your own locale-specific properties file for internationalizing the Craft Interface tool. The locale-specific properties can be edited using the I18N Editor tool.

### 6) Context-sensitive help file (tl1craftinterface\_csh.xml)

This file contains short description about each component used in the Craft Interface UI. When the context-sensitive icon is placed on a particular component, the description about that component is displayed in a small window.

### 7) TL1AppletInfo.html

This file is used only in the case of Craft Interface Applet and is created when you run the **StartTL1AppletServer** script. This file contains information about the RMI port which is used for doing all the client-server transactions.

## 6.15.2.4 How to Configure TL1 Craft Interface?

- Session
- Message
- User Interface
- Log File

When a TL1 Craft Interface shows up, it always gets loaded with the default properties configured. These default properties can be changed based on your requirements. The Options Window allows you to do this. You can open this window by selecting the **Options** button from the Tools menu.

The Options Window is split into five categories: **Session**, **Message**, **User Interface**, and **Log File**. Each option has its own default properties. The default properties are stored into **tl1craftinterface.config** file present under <Web NMS Home>/conf directory.

After editing the default properties, click the **OK** or **Apply** button to save the changes. Click the **Cancel** button to discard the changes.

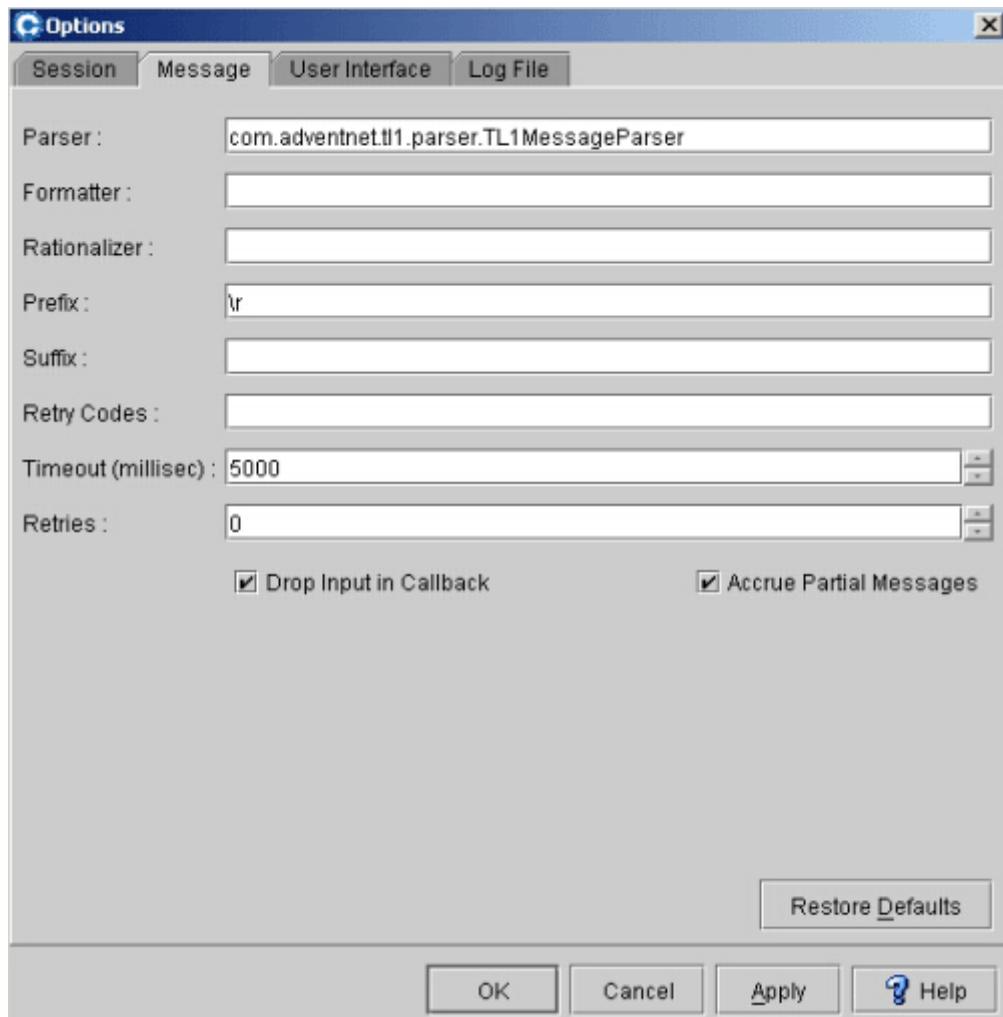
### Session option

The Session option will let you modify the parameters pertaining to the TL1 Session, such as Transport, Mode, Keep Alive, Connection Handler, etc.

| Parameter                 | Description                                                                                                                                                                                                                               |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mode</b>               | Normal or Craft. In Normal mode, messages are processed, queued up and sent to the application. But in Craft mode, messages are given without any processing.                                                                             |
| <b>Transport</b>          | Represents the connection parameters for each transport (i.e. TCP, Telnet, and Serial).                                                                                                                                                   |
| <b>Connection Handler</b> | Represents the interface <b>ConnectionHandler</b> . Users can perform any device-specific tasks by plugging in their own custom class that implements this interface. This interface is invoked while opening and closing the connection. |
| <b>Keep Alive</b>         | This option if enabled helps you to maintain connection with the device by sending messages periodically. You can set the TL1 message and the time interval.                                                                              |

### Message option

The Message option will let you modify the default properties related to TL1 Message, such as Parser, Formatter, Rationalizer, Prefix and Suffix of each message, Timeout and Retries, etc. The default properties are shown in the image.



| Parameter                           | Description                                                                                                                                                                                                                                                                                               |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parser</b>                       | Represents the interface <b>TL1Parser</b> . This interface parses the TL1 messages and generates message objects. By default, <b>com.adventnet.tl1.parser.TL1MessageParser</b> is implemented. You can also plug in your own parser implementation.                                                       |
| <b>Formatter</b>                    | Represents the interface <b>MessageFormatter</b> . This interface allows users to format specific TL1 messages. Users can plug in their own formatter by implementing this interface. By default, its value is <b>null</b> .                                                                              |
| <b>Rationalizer</b>                 | Represents the interface <b>MessageRationalizer</b> . This interface allows users to upgrade messages based on the XML message definitions (command set) or filter specific TL1 messages. Users can plug in their own rationalizer by implementing this interface. By default, its value is <b>null</b> . |
| <b>Prefix and Suffix</b>            | Append special strings at the start and end of each TL1 message. This is optional and may not be applicable for all devices. The default prefix is \r and the suffix is <b>null</b> .                                                                                                                     |
| <b>Timeout</b>                      | Represents the timeout value of each request. By default, the timeout is <b>5000</b> .                                                                                                                                                                                                                    |
| <b>Retries</b>                      | Represents the retries value that session has to do for each request. By default, the retries is <b>0</b> .                                                                                                                                                                                               |
| <b>Partial Message Accumulation</b> | Option to provide or accumulate partial messages received from the device. If set to true, all partial messages are accumulated and given only after receiving a response with proper terminator (;).                                                                                                     |



**Note:** The special characters, **\r**, **\n**, **\f**, **\b**, **\t** are supported for prefix and suffix fields. Other characters are interpreted as specified.

You can change the default properties by editing the appropriate fields.

### User Interface option

The User Interface option will let you modify the default properties of the Craft Interface, such as color, look and feel, etc. You can change the default properties by selecting the appropriate fields. You can also modify the default location of the files used by the Craft Interface, such as Help Documentation and Data files. You can modify the existing location by selecting the ... button.

### Log File option

The Log File option will let you modify the default log configuration, such as File Name pattern, Time Stamp enable, Rollover details, etc.

| Parameter                | Description                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pattern</b>           | Pattern indicates the order in which the log file name must exist.<br>%n represents the log file name.<br>%d represents the date at which the log file is generated.<br>%t represents the time at which the log file is generated.<br>%c represents the log file count generated for that particular connection.<br>The date and time are optional in pattern. |
| <b>Time Stamp</b>        | Represents the time at which the log record is created.                                                                                                                                                                                                                                                                                                        |
| <b>Append</b>            | Appends the log information to the same log file that was previously used by this connection.                                                                                                                                                                                                                                                                  |
| <b>Rollover Size</b>     | Maximum size of a log file after which a new log file will be created. You can give a value of 0 if you do not want log files to be created based on size. The size should be given in bytes.                                                                                                                                                                  |
| <b>Rollover Time</b>     | Time that must be specified after which a new log file will be created. The time should be given in the hh-mm-ss format.                                                                                                                                                                                                                                       |
| <b>Rollover Count</b>    | Maximum number of log files to be created for a specific device connection.                                                                                                                                                                                                                                                                                    |
| <b>Rollover Interval</b> | Interval that must be specified after which a new log file will be created. The interval should be given in milliseconds                                                                                                                                                                                                                                       |

## 6.15.2.5 Internationalization

The TL1 Craft Interface tool supports Internationalization and allows you to work with both application and applet in various languages without doing any change to the source code. The localized content can be added easily and the same executable can be run worldwide. All the textual elements such as GUI component labels, buttons, etc. can be made suitable to the locale (combination of specific language and country) of the user.

This section will let you know how to,

- Create a properties file for Internationalization
- Configure the Locale and Properties File Path

### Create a properties file for Internationalization

The default properties file (**tl1craftinterface\_i18n.properties**) present under <Web NMS Home>/conf contains a list of words used in the TL1 Craft Interface. This file can be used as a template for creating your own locale-specific properties file. This template contains English string of all the GUI labels and messages. You can create locale-specific properties file through the I18NEditor tool.

The **tl1craftinterface\_i18n.properties** file has to be copied to a specific locale file. For example, to display the TL1 Craft Interface in chinese language, the **tl1craftinterface\_i18n.properties** has to be copied as **tl1craftinterface\_i18n\_zh\_CN.properties** file. The language and the country should be represented by standard two-letter codes (zh - Chinese and CN - China).

By default, the locale-specific file contains English string as keys. The developer has to write the equivalent string of the chosen language and country to this file as value against the equivalent key. This will enable the Craft Interface to display the custom string instead of English string. For text whose corresponding locale-specific string is not given, English string is used. If the specified locale file is not present in the specified directory, the default properties file, **tl1craftinterface\_i18n.properties** will be searched and loaded.

The format given in the **tl1craftinterface\_i18n.properties** file should not be altered. The default English string are provided with the escape sequence characters. For example, the string "TL1 Craft Interface" is provided as "TL1\ Craft\ Interface". However the equivalent string (of the chosen language) need not have the escape sequence included.

### Configure the Locale and Properties file path

The Internationalization feature in TL1 Craft Interface will take effect only if the locale and property file path are set before starting the application or applet. These parameters can be changed by editing the **TL1CraftInterface** (.bat/.sh) file under <Web NMS Home>/bin/browsers directory. The default parameters for these entries is shown below.

```
java com.adventnet.tl1.tools.craftinterface.CIMainScreen -
NMS_RESOURCE_DIRECTORY ./conf -RESOURCE_PROPERTIES
tl1craftinterface_i18n -RESOURCE_LOCALE en_US
```

| Argument                | Description                                                                | Default Value          |
|-------------------------|----------------------------------------------------------------------------|------------------------|
| -NMS_RESOURCE_DIRECTORY | The directory or path from where properties file has to be fetched         | conf                   |
| -RESOURCE_PROPERTIES    | Name of the properties file                                                | tl1craftinterface_i18n |
| -RESOURCE_LOCALE        | Indicates the locale string. This represents the language and country code | en_US                  |



**Note:** In Applet mode, following entries should be changed in the **TCIApplet.html** present under <Web NMS Home> to support Internationalization of TL1 Craft Interface tool.

For example,  
<PARAM NAME="RESOURCE\_PROPERTIES"  
VALUE="tl1craftinterface\_i18n\_en\_us">  
<PARAM NAME="NMS\_RESOURCE\_DIRECTORY" VALUE="conf">

## 6.15.2.6 Re-branding TL1 Craft Interface

By default, AdventNet branding appears in the UI of TL1 Craft Interface. The re-branding feature offered by this tool allows you customize the user interface to display your own company information. Rebranding lets you change:

- Company logo in the place of AdventNet logo
- Tool name in the application
- Frame Icon
- Splash Image at Startup
- Toolbar, About and Right Panel images
- Message Color
- Organization URL
- Progress Bar Foreground and Background color

### How to Modify the Settings

| Re-brandable Feature                                      | Where it appears in the UI                                                                              | Notes                                                                                                                                                                     |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Company Logo and URL                                      | Present in the right corner of the toolbar                                                              | Modify the property value of <b>Company -&gt; url</b> and <b>Company -&gt; logo</b> in the <b>tl1craftinterface.config</b> file.                                          |
| Tool name                                                 | Present in the Application title bar                                                                    | This can be changed by modifying the value of TL1 Craft Interface field in the <b>tl1craftinterface_i18n.properties</b> file present under <Web NMS Home>/conf directory. |
| Frame Icon                                                | Present in the left corner of the title bar                                                             | Modify the property value of <b>UI:Images:frameicon</b> in the <b>tl1craftinterface.config</b> file.                                                                      |
| About Image                                               | Invoked when you select the <b>Help -&gt; About</b> button                                              | Modify the property value of <b>UI:Images:abouttoolicon</b> in the <b>tl1craftinterface.config</b> file.                                                                  |
| Splash Image                                              | Invoked when the application is started                                                                 | Modify the property value of <b>UI:Images:splashicon</b> in the <b>tl1craftinterface.config</b> file.                                                                     |
| Right Panel Image (root, file, module, request, glossary) | Invoked when you select the corresponding node in the Message Tree                                      | Modify the property value of the corresponding entry in the <b>UI:Images:RHPPanel</b> in <b>tl1craftinterface.config</b> file.                                            |
| Toolbar Icons                                             | Present just below the menu bar                                                                         | Modify the property value of <b>UI:Images:ToolBar:*</b> in the <b>tl1craftinterface.config</b> file.                                                                      |
| Progress Bar Foreground and Background color              | Invoked when the application is started                                                                 | Modify the property value of <b>SplashScreen:ProgressBar:*</b> in the <b>tl1craftinterface.config</b> file.                                                               |
| Message Color                                             | This indicates the color of each message, request, response and notification in the response text area. | You can modify it from the UI by selecting <b>Tool -&gt; Options -&gt; User Interface</b> .                                                                               |

## 6.15.3 CLI Browser: An Introduction

- 
- Overview
  - Features of CLI Browser
  - Starting CLI Browser
  - What this section explains
- 

### Overview

The AdventNet CLI Browser is a GUI experienced network management application that supports Command Line Interface and can be used to manage network devices. You can use CLI Browser to communicate with network devices such as routers, switches, remote machines, and others. It works based on a command template that is used to generate CLI commands. This can also be used to execute scripts, terminal transformation, and others. The CLI Browser can be customized according to your requirements.

### Features of CLI Browser

The key features of CLI Browser are given below :

- Connecting devices through Telnet and Serial (RS232)
- Loading XML-driven Command Set
- Launching Python and BeanShell scripts
- Terminal transformation
- Multiple prompt
- Support for control characters

### Starting CLI Browser

Execute the **CLIBrowser.sh/.bat** file from the <Web NMS Home>/bin/browsers directory. You can also start CLI Browser from **Web NMS Launcher -> Administrator Tools**.

XML-driven Command Set and Data Set plays a vital role in generating CLI commands. You can use the DTD for **commandset** and **dataset** that are available in <Web NMS Home>/ccs directory as a reference to generate commands. We provide sample Command Set and Data Set files for few UNIX and Show Commands.

The AdventNet CLI Browser has the capability to load and use different files having different set of Input messages. The Input CLI Command is the indication of what operation is being done. You can load and unload multiple files.

To communicate with network devices, start the CLI Browser, connect any device, and select a valid CLI command in the input message field present in the right frame. The response can be received from the device after sending the command.

This section explains:

---

- Overview
- Connecting Devices
- Loading Files

- Configuring Message Parameters
  - Sending CLI Command
  - Executing Scripts
  - Terminal Transformation
  - Enabling Special Characters
  - Debugging Message
  - Command Generation
  - Internationalization
-

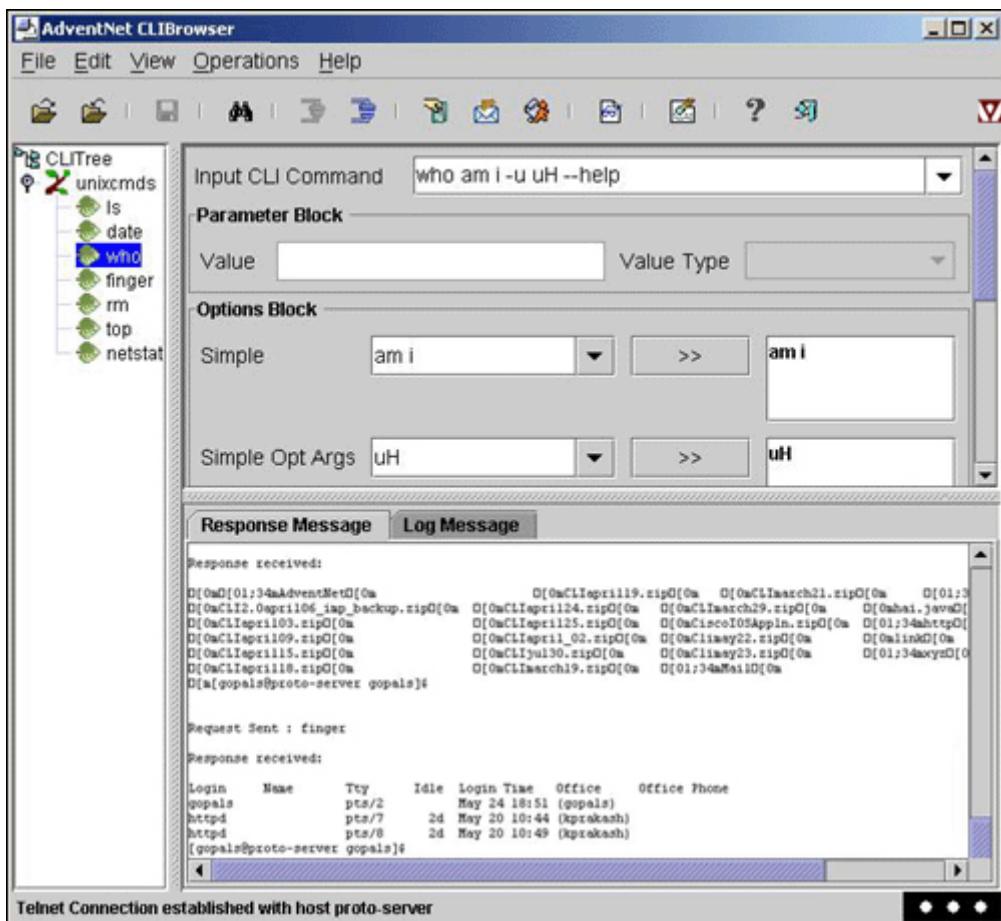
## 6.15.3.1 Overview

- How does the CLI Browser look like?
- Menu Bar
- Toolbar
- Keyboard shortcuts

### How does the CLI Browser look like?

The primary window of AdventNet CLI Browser is made up of two frames. The left frame contains the CLI Tree that is used to load the CLI commands. The right frame contains details about the selected CLI command, parameters, command options, and text area to display the response received from the device.

AdventNet CLI Browser view shown below is a self-explained complete picture of CLI-based communication with devices.



## Left Frame

- CLI Tree - To select various CLI commands to be sent to devices. The commands are generated by loading the Command Set / Data Set files which are in the form of XML.

## Right Frame

- Text field that shows the CLI command being selected.
  - Text field to display the details of the parameter block. The parameter block consists the Parameter Value, which can be modified.
  - Text fields to display the details of the options block. The options block consists of the following and these values can be updated in command.
    - Simple Options
    - Simple Options with Arguments
    - Long Options
    - Long Options with Arguments
  - A Text area to display the Description of the input message.
  - A Tabbed Text area to display the Response and log messages from the device.
- 

## Menu bar

The Following menus are available in CLI Browser.

### Main Menus

#### File Menu

- **Load** - To load the XML file.
- **Unload** - To unload the file from Tree.
- **Save** - To save the current default values into specified default file.
- **Save As** - To save the current default values into a file with a new name.
- **Exit** - To quit from CLI Browser.

#### Edit Menu

- **Settings** - To modify the browser configuration settings, i.e. message parameters such as setting the request Timeout, message suffix and message prompt, and others.
- **Find Node** - To Search for a particular node in the Tree.

#### View Menu

- **Response Tab** - To set the Font type, Background color and Foreground color of the Response Text Area.
- **Toolbar** - To display or hide the toolbar.
- **Option Block** - To display the various options for a command. The options are simple and long with and without arguments

#### Operations Menu

- **Connect** -To open a connection with the specified device.
- **Disconnect** - To disconnect the device from the browser.
- **Send** - To send the Input message to the device.

- **Execute Script** - To execute the Python and BeanShell Scripts.
- **Enable Special Char** - To enable the special characters typically used for communication and device control.
- **Enable Transformation** - To enable the terminal transformation.
- **Clear** - To clear the response message box.
- **Debug Messages** - To debug the messages.

#### Help Menu

- **Contents** - This shows the AdventNet CLI Browser help documentation.
- **About** - This shows the about screen of CLI Browser.

#### Popup Menus

Apart from the main menus, CLI Browser also has two pop-up menus that pop-up in the text area and Tree panel respectively. Right clicking of the mouse button in the particular window will make these menus pop up In the text area of the Response tab, following menus are available.

- **Settings** - To set the Font type, Background color, and Foreground color of the Response Text Area.
- **Copy** - To copy the selected text.
- **Paste** - To paste the copied text in to text area.
- **Save As** - To save the selected text to a file.
- **Clear All** - To clear all the text that is printed in the text area.
- **Find Node** - To find a node in the Tree panel.

#### Toolbar

The Toolbar allows you to perform actions quickly using the mouse. CLI Browser allows you to show/hide the Toolbar. Following Toolbar options are available with CLI Browser.

| Button | Description                                                               |
|--------|---------------------------------------------------------------------------|
|        | Loads the Command Set and Data Set file, which contains the CLI commands. |
|        | Unloads the Command Set and Data Set from CLI Tree.                       |
|        | Saves the changes made in Data Set file.                                  |
|        | Searches a particular node or command in the CLI Tree.                    |
|        | Connects the device.                                                      |
|        | Disconnects the device.                                                   |
|        | Configures the CLI command.                                               |
|        | Sends the selected CLI command to the device.                             |
|        | Executes the scripts in Python and BeanShell.                             |
|        | Debugs the response.                                                      |
|        | Decodes the response.                                                     |
|        | Clears the response text area.                                            |
|        | Displays the help documentation.                                          |
|        | Exits the CLI Browser.                                                    |

## Keyboard Shortcuts

Keyboard shortcuts accomplish the common tasks quickly, which are frequently used. Shortcut keys help to work faster.

| Shortcut Key | Action                                        |
|--------------|-----------------------------------------------|
| Ctrl+O       | Load the file                                 |
| Ctrl+U       | Unload the file                               |
| Ctrl+S       | Save the file                                 |
| Ctrl+Shift+S | Save As the file                              |
| Alt+F4       | Exit the file                                 |
| Ctrl+Shift+T | Set the message parameters                    |
| Ctrl+F       | Find the node                                 |
| Ctrl+Shift+C | Connect                                       |
| Ctrl+Shift+D | Disconnect                                    |
| Ctrl+N       | Send                                          |
| Ctrl+X       | Execute script                                |
| Ctrl+L       | Clear the response and log messages           |
| Alt+D        | Debug response.                               |
| Ctrl+Shift+B | Change background color of Response Text Area |
| Ctrl+Shift+G | Change foreground color of Response Text Area |
| Ctrl+T       | Change font of Response Text Area             |
| F1           | Help                                          |

### Shortcut Keys in Find dialog box:

| Shortcut Key | Action                                                 |
|--------------|--------------------------------------------------------|
| Alt+ N       | Find what                                              |
| Alt+ F       | Find next occurrence of the node name in tree          |
| Alt +L       | Close the dialog box                                   |
| Alt+ C       | Search for the specific node matching the case entered |
| Alt +W       | Search for the specific node matching the word entered |

## 6.15.3.2 Connecting Devices

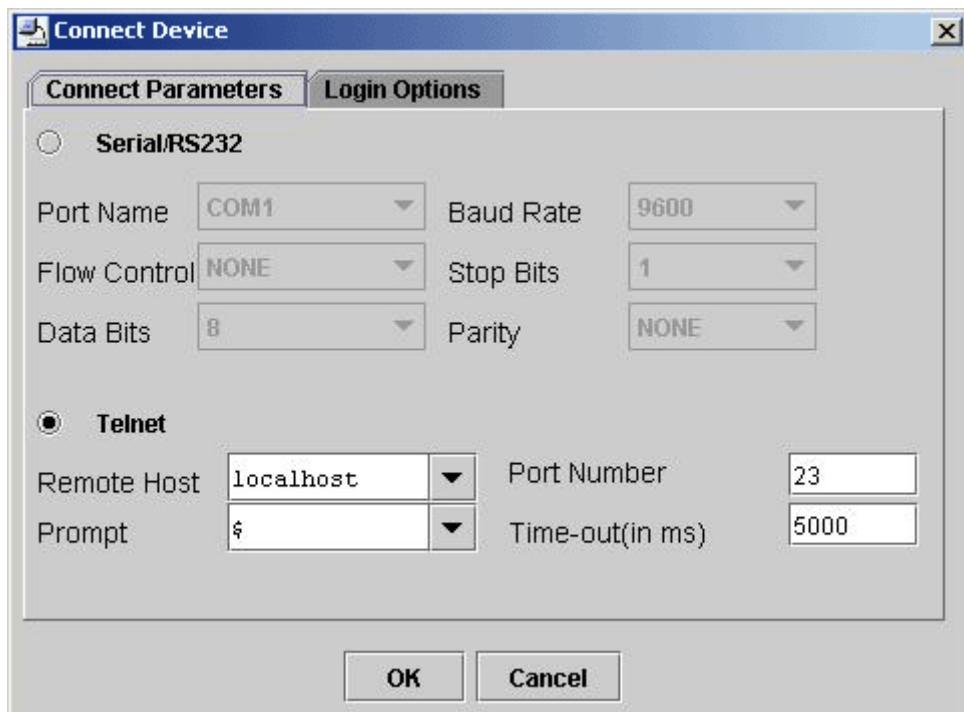
- Overview
- Connect Parameters
  - Serial/RS232
  - Telnet
- Login Options

### Overview

The network devices can be connected through **Serial/RS232** or **Telnet**. Use Serial/RS232, if you are connecting devices using a cable, which are at a proximate distance. The remote devices can be connected using Telnet. Before connecting device, set various connection parameters and login options.

### Connect Parameters

The devices can be connected through Telnet or Serial port.



### Serial/RS232

The serial port sends and receives bytes of information in a serial fashion - one bit at a time. These bytes are transmitted either using a binary format or using a text format.

#### Port Name

The serial port is called COM1, COM2, etc. in DOS/Windows and dev/ttyS0, dev/ttyS1, etc. in UNIX machines. Select a suitable port or add a new port.

## Stop Bits

Stop bits are added to the serial communication protocol to allow the receivers to synchronize on the characters being sent. It can be set as 1 or 2.

## Data Bits

The data bits transferred through a serial port may represent device commands, sensor readings, error messages, and others. The data can be transferred either as binary data or as ASCII data. Most serial ports use between five and eight data bits. Binary data is typically transmitted as eight bits. Text-based data is transmitted either as seven bits or as eight bits.

## Parity

The parity can be set to none, even, odd, mark, or space. With odd parity, the parity bit is selected so that the number of 1-bits in a byte, including the parity bit, is odd. Even parity works in a similar manner with all legal bytes including the parity bit having an even number of 1-bits.

For mark parity, the parity bit is always a one-bit. For space parity it's always a zero-bit. Mark or space parity only wastes bandwidth and should be avoided if possible. "No parity" means that no parity bit is added.

## Baud Rate

The "baud rate" is data transmission rate (bits/second). Usual transmission speed ranges from 9600 and 19200 BPS that are used in most automation and console applications to 115200 BPS used by the fastest modems.

## Flow Control Mode

It is the mechanism that regulates the flow of data between two devices. Modems typically have two methods of flow control: software flow control (XON/XOFF) and hardware flow control (CTS/RTS).

## Telnet

### Remote Host

This parameter specifies the system/device for which the connection has to be established. Typically you can set it to "localhost" if you wish to establish a connection with your own system (provided your system supports Telnet, i.e. it is running a Telnet server). Change the host name accordingly if you wish to connect with a different host.

### Port Number

For Telnet, this has the value 23 (the standard telnet port). Because this is the default value, you need not even set it. Only if all the above parameters are correct can the login Succeed and the CLI session can be established.

### Prompt

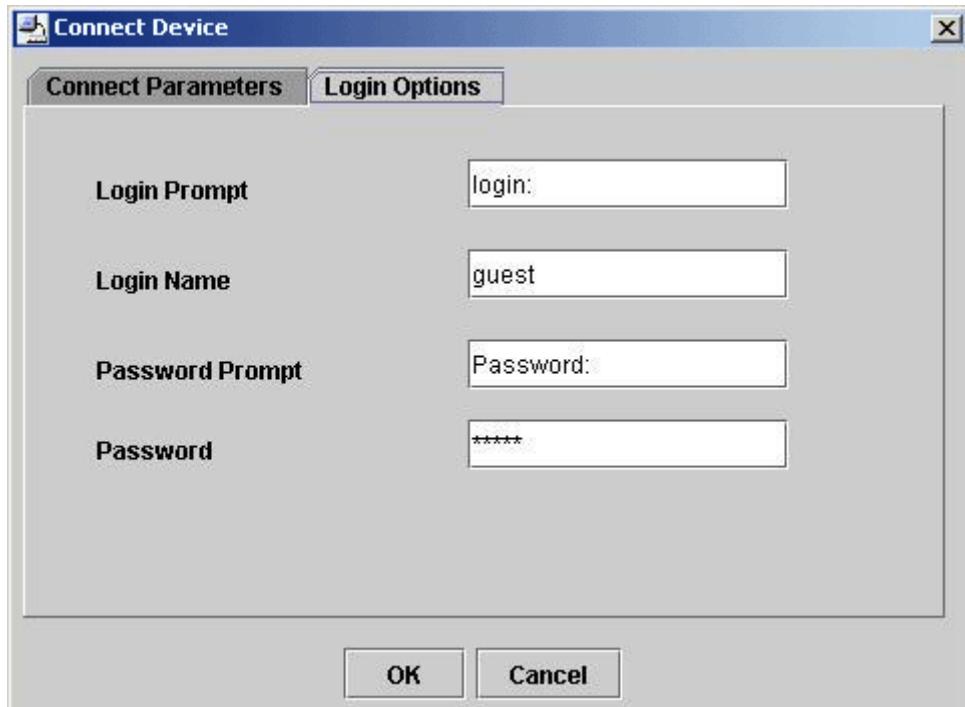
The prompt is the string issued by the system/device after a successful login for getting the commands. Typically this is a "\$" or "#". Check the prompt that is issued by your system/device. This is set as "\$" assuming the command prompt is "\$". Change accordingly if this differs on your system.

## Login Timeout

The Login Timeout is the time elapsed after which the connection with CLI device has to be reset. This is set as 5000 milliseconds by default.

## Login Options

Login Options allows you to set Login Prompt, Password Prompt, Login Name, and Password.



### Login Prompt

This is the prompt issued by the remote system or device for getting the Login name or user name. Typically this is "**login:**" for UNIX systems. Please make sure whether this is the prompt issued by your system/device. This can be checked by establishing connection through Telnet to the device using the standard telnet command. Change accordingly if this option differs.

### Password Prompt

This is the prompt issued by the remote system for getting the password for the Login name provided when prompted for login: Typically this is "**Password:**" for UNIX systems. You can also check whether this ("Password") is the prompt issued by your system/device. Change accordingly if this option differs.

### Login Name

This is the user name or Login name that is present in the system. Check whether the user name you are setting exists on the remote system. This is set as "guest" assuming the user guest exists in the system. Change accordingly if this differs on your system.

### Password

The password for the user name. Make sure that the password that is set is correct. This is set as "guest" assuming the password for user guest is "guest". Change accordingly if this differs in your system.

|                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>Note:</b> <ul style="list-style-type: none"><li>• If you are connecting the device using the Serial port on Windows and Solaris, make sure to set the comm.jar in the jdk CLASSPATH, which can be downloaded from <a href="http://java.sun.com/products/javacomm">http://java.sun.com/products/javacomm</a>. Please refer to the instructions given in javacomm20-win32 for details. For Linux, OS, please install JCL, which is available at the following URL : <a href="http://www.interstice.com/kevinh/Linuxcomm.html">http://www.interstice.com/kevinh/Linuxcomm.html</a></li><li>• Provide connect parameters and login options for Telnet when you are starting the CLI Browser from Web NMS Launcher.</li></ul> |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**To Connect the Devices**

- Click  or the **Connect** in Operation menu.
- Select the connection type either **Serial/RS232** or **Telnet**.
- Set the **Connection Parameters** for respective type of connection. For Serial/RS232 set the Serial Port parameters and for Telnet set Remote Host, Port Number (Telnet Port), Delimiter, Login Timeout (in milliseconds).
- Set the **Login options** if Login options are required.
- Click **OK** to establish connection with the device.

### 6.15.3.3 Loading Files

CLI Browser supports loading CLI commands to be sent to the devices. The commands are generated using Command Set and Data Set, which are written using XML. You have to load XML files for Command Set as well as Data Set in CLI Tree, which is in the left side panel of CLI Browser.

Command Set file is used to define a set of command templates for a particular device. It consists of all the possible commands (configuration, monitoring, and others) for a particular device. For each Command Set, a Data Set is associated that contains all the data definitions needed for the commands. The structure of the XML file is explained in detail in the **Command Generation** page.

To load an XML file in CLI Browser, click  or select **Load** menu item from the **File** menu. This opens a Message Set Configuration dialog. The dialog contains a table, which contains the loaded XML files and their corresponding data files.

You have a privilege to load multiple XML files, but you can send only one command from the Browser at a time to a CLI device. To add a new XML file into CLI Browser, click **Add** button. This opens another configuration dialog. Click **Browse** button corresponding to Command Set and (or) Data Set to load a Command Set and (or) Data Set file. After selection, Click **OK** to accept file loading or **Cancel** to cancel the file loading. Once an XML file is selected in configuration dialog, it gets added in the table along with data file.

In order to change a data file for a particular XML file, you must select the data file first and click **Modify** button to change the data file loaded.

The XML file can be browsed by selecting the required file from directory.

To Unload an XML file from the Browser, click  on the Toolbar or **Unload** menu item from the **File** menu. This opens a dialog that displays the files previously loaded. You can select a particular file from combo box and click **Unload** button to unload the file from the list. This also removes file from the table in load configuration dialog.



**Note:** Multiple Command Set and Data Set files can be loaded into CLI Browser, but only one message can be sent to the device at a time.

#### To Load Command Set and Data Set

- Click  or **Load** from File menu.
- Click **Add** to load the Command Set and Data Set files.
- Click **Browse** and select the corresponding Command Set and Data Set files to be loaded.
- Click **Modify** to change the data file loaded (if required).
- Click **OK** to accept file loading or **Cancel** to cancel the file loading.

## 6.15.3.4 Configuring Message Parameters

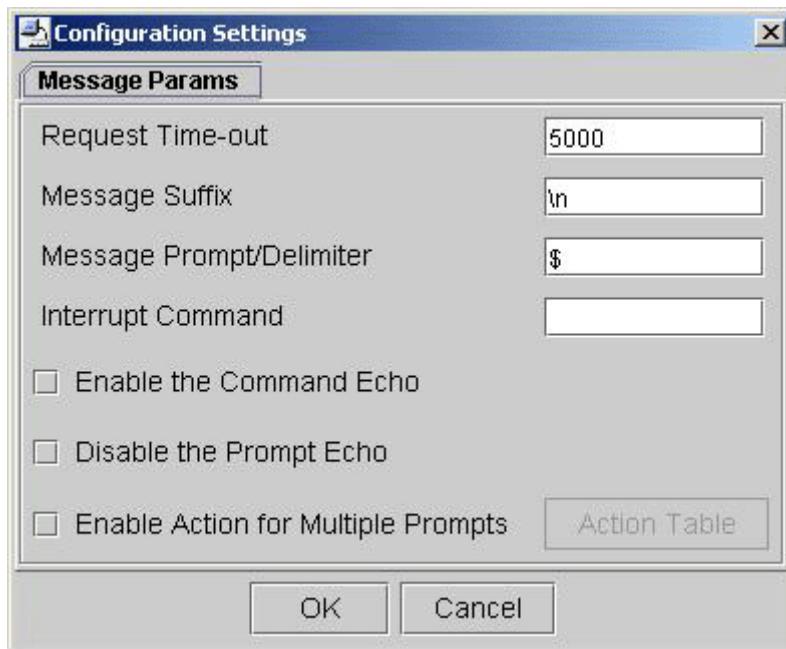
- Overview
- Set the Request Timeout
- Set the Message Suffix
- Set the Message Prompt
- Interrupt Command to Be Sent
- Enable the Command Echo
- Disable the Prompt Echo
- Enable Action for Multiple Prompts

### Overview

Message configuration is one of the important tasks while sending a CLI command to device. You can do message configuration for the following reasons.

- Message suffix differs from device to device. It may be `\n` for UNIX OS, whereas `\r` for Windows OS.
- The prompt varies from device to device. In general, the prompt for UNIX machines is `$`, `#`, or some other, whereas for Windows it may be `:>`. If you are connecting devices such as routers the prompt may be `>` in user mode, whereas `#` in privilege mode. Hence you need to change the prompt to send CLI commands to devices such as routers in different modes.
- Sometimes, you may need to increase the timeout after establishing the connection, as some responses may need more time to receive the response.
- You may need to send different prompts for receiving the response from the device that can be addressed by enabling the action for multiple prompts.

The following message parameters can be configured before sending messages through the CLI Browser :



## Request Timeout

Set the timeout in milliseconds for the request message. If the response is not received within the time, a timeout occurs.

## Message Suffix

Set the message suffix for the message. This will be appended at the end of each message sent.

## Message Prompt

This is the Prompt/delimiter for the command being sent. The default Message Prompt will be set according to Prompt/Delimiter set in the Connection Parameters while trying to establish connection with the remote host. It can be configured according to the Prompt/Delimiter expected in the response for the input command.

## Interrupt Command

If the response is not received within the timeout, the interrupt command will be sent to the device. It can be set in such a way that the command prompt returns and the next command can be sent.

## Enable the Command Echo

It is to indicate whether to enable or disable the command echoing. By enabling the CommandEcho, the command that is sent will be displayed in the received response.

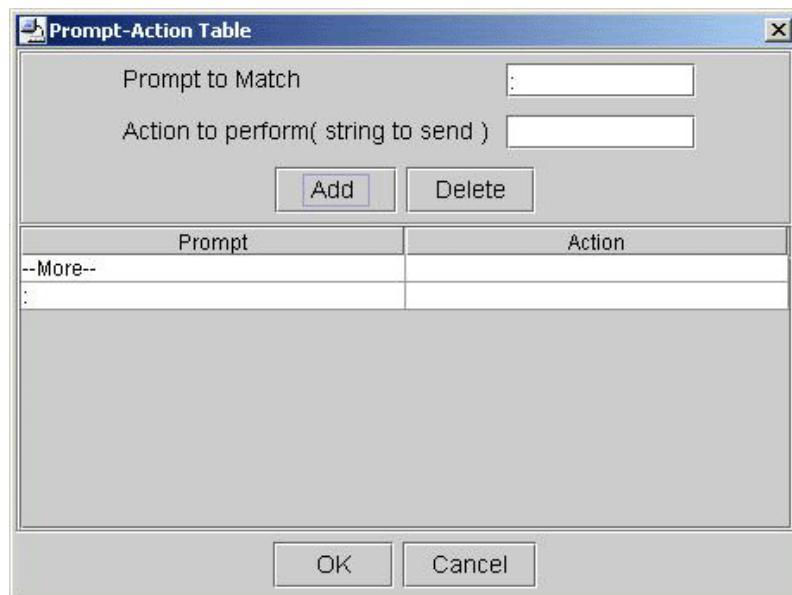
## Disable the Prompt Echo

It is to indicate whether to disable or enable the prompt echoing. By disabling the PromptEcho the prompt will not be displayed. For this function to work set the whole command prompt in the text field where the Message Prompt/Delimiter is set.

## Enable Action for Multiple Prompts

Set the possible multiple prompts and the corresponding actions. A device can set the prompts after executing a command. In general, when the response does not fit into the screen, it prompts for an action from user to receive the remaining response.

For example in UNIX machines when commands such as `man` is sent to the device, it prompts ":" after receiving a block of response and you have to send "space" from Keyboard as a corresponding action.



After enabling the action for multiple prompts, you can add the prompt and corresponding action to perform. All the prompts and corresponding actions are added in a table. While sending CLI command to the device, if it encounters any of the prompts the corresponding action will be sent to the device.

#### To Configure the Message Parameters

- Click  in Toolbar or **Settings** from Edit menu.
- To display the command that is sent in Response Received Tab, check the **Enable the CommandEcho** check box.
- Check/uncheck the **Disable CommandEcho** check box to hide/display the command prompt in Response Received Tab. For this function to work set the whole command prompt in the text field where the Message Prompt/Delimiter is set.
- Set the **Request Timeout** in milliseconds for receiving the response (timeout occurs and an exception is thrown if response is not received within that period).
- Set the **Message Suffix** to be appended to each message sent (default is \n).
- Set the **Message Prompt** according to the Prompt/Delimiter expected in the response for the input command sent.
- Enable **Action for Multiple Prompts** and store the prompt and corresponding action.
- Click **OK** to accept or **Cancel** to cancel the configuring message parameters.

## 6.15.3.5 Sending CLI Command

- 
- Overview
  - Modifying the Parameter Value (Optional)
  - Modifying the Option Value (Optional)
- 

### Overview

Sending a CLI command involves primarily two tasks. First selecting a suitable command and then sending it to device. Select the command and modify the parameters and options for a specific input command if you need the changes. You can also send commands directly by entering a suitable command from the Input CLI Command.

Select a command from CLI Tree. The CLI commands may have various parameters and options. You can modify the parameters from the parameter block. After modifying the parameters if the focus is lost from parameter block, it automatically updates the input CLI command.

### Modifying the Parameter Value (Optional)

1. Make changes, if required to **Param Value** column of the **Parameter Block** in the right frame of CLI Browser.
2. Click  on the Toolbar or select **Save** menu item from the **File** menu to save the default values into Data Set file.



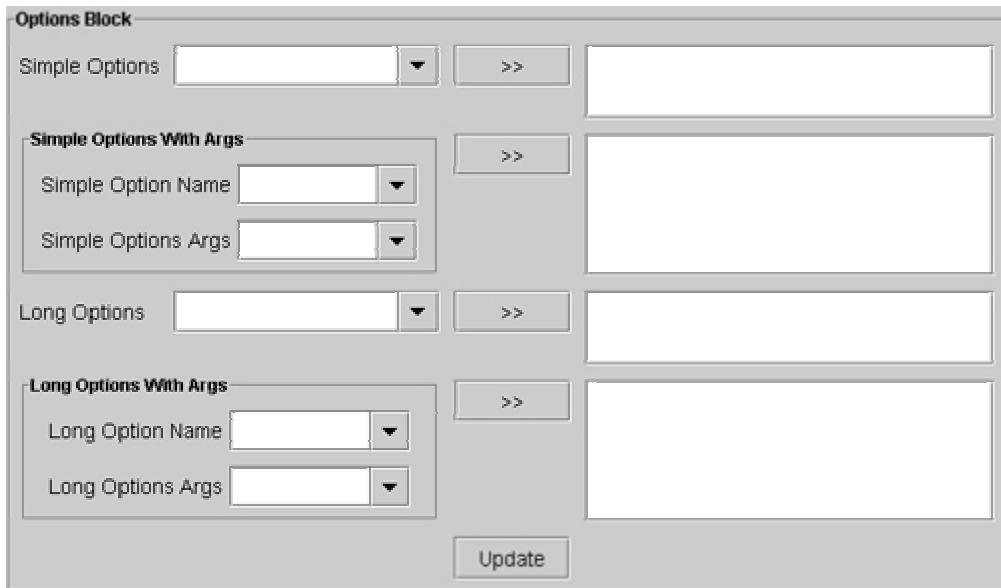
| Param Name    | Param Value | Param Type | Select Option                       |
|---------------|-------------|------------|-------------------------------------|
| compiled      | \$          | Value      | <input checked="" type="checkbox"/> |
| access-listid | 0           | Value      | <input type="checkbox"/>            |

**Update**

Each command may have various options. CLI Browser has an Option block that allows you to update the options for a command. The Option block, by default, is in disabled mode. You can enable this if it is required. Following options are available in Option block:

### Modifying the Option Value (Optional)

1. Make changes, if required to **Value** text field of the **Option Block** in the right frame of CLI Browser.
2. Click **Update** to append the command to the options.



## Simple Option

`ls -l`

To get a long listing of the contents of the current directory. In this example, "ls" is the command name, "-l" is an option that tells "ls" to create a long, detailed output. Here the option is simple as it is has prefix (i.e. delimiter) "-".

## Simple Option with Arguments

`ls -l /tmp`

To get a long listing of the contents of the /tmp directory. In this example, "ls" is the command name; "-l" is an option that tells "ls" to create a long, detailed output, and "/tmp" is an argument naming the directory that "ls" is to list.

## Long Option

`ls --all /tmp`

To get an "all" listing of the contents of the current directory. In this example, "ls" is the command name; "--all" is an option that tells "ls" to create a all, detailed output. Here the option is long as it is has prefix (i.e. delimiter) "--".

## Long Option With Arguments

`ls --all /tmp`

To get an "all" listing of the contents of the /tmp directory. In this example, "ls" is the command name, "--all" is an option that tells "ls" to create an all, detailed output; and "/tmp" is an argument naming the directory that "ls" is to list.

### To Send CLI Commands

- Select a command from CLI Tree.
- Modify the parameter value in Parameter block.
- Update the options in Option block.
- Click  in Toolbar or **Send** from Operations menu.

## 6.15.3.6 Executing Scripts

- 
- Overview
  - Browsing the Script File
  - Executing Scripts with Arguments
- 

### Overview

AdventNet CLI Browser extensively supports executing scripts which are used to simplify the complex CLI Device configuration tasks. You can execute **Python** and **BeanShell** scripts with single line as well as script written in a file with arguments.

### Browsing the Script File

AdventNet CLI API provides Python and BeanShell scripts to establish the connection and communicate with devices. You can use sample scripts **CliSyncApp.py** and **CliSyncApp.bsh** files available in <Web NMS Home>/examples/cli/scripts/ directory and receive output into response text area.

### Executing Scripts with Arguments

You can execute scripts with arguments. For example, if you are connecting to a device you can specify the host name, login name, password, and command text box with space separated as shown below:

#### To Execute the Scripts

- Click  in Toolbar or **Execute Script** menu item from Operations menu.
- Select a suitable scripting language. You can select either **Python** or **BeanShell**.
- **Browse** the script, open \*.py file for python and \*.bsh for BeanShell
- Click **OK** to execute the script. You can view the output either in console or Response Text Area.

### 6.15.3.7 Terminal Transformation

CLI Browser can be used to enable terminal transformation. Terminal transformation can be used for emulating different types of terminals such as vt100, vt320, IBM and others.

The transformation table can be in the form of either XML or text. A sample **TransformationTable.xml** is available in <Web NMS Home>/conf directory. It consists of the following tables and allows you to add more tables.

- vt100 to IBM
- vt100 to Null

#### To Enable Transformation

1. Enable Transformation from Operations menu.
2. Browse transformation table.
3. Select the required transformation table.
4. Click **OK** to enable transformation.

### 6.15.3.8 Enabling Special Characters

CLI Browser supports sending the special characters such as control characters and non-printable characters that are typically used for communication and device control.

For example, if you are sending command such as "ping" you can stop the process by sending ^C (from keyboard Shift+^+C) that interrupts the response and returns to the command prompt.

#### To Send Special Characters

1. Click **Enable Special characters** from operations menu.
2. In Input CLI Command, enter Shift+^+C (If ^C character has to be sent to the device.)
3. Click  or Send menu.

## 6.15.3.9 Debugging Message

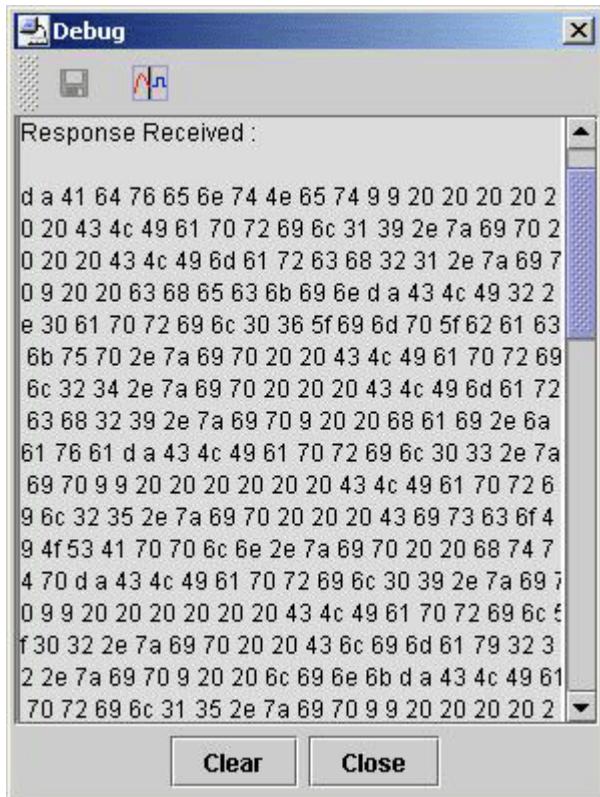
- Invoking the Debugging Window
- Invoking the Decoder Window
- Performing the Decoding Operation

The CLI Browser provides facility to view the debug output of the CLI operations.

### Invoking the Debugging Window

1. Click the  or select **Debug** from the View menu. You can also use the shortcut key combination Alt+D. This would invoke the Debug window.
2. As long as this debug window is opened, debugging is turned on and the debugging output is displayed. When this window is closed, debugging is turned off.

The image below depicts a debug window.



3. Click the  in Debug window to switch to Decoder Window.

### Invoking the Decoder Window

1. To switch from the debug window to the decoder window, click the decoder icon. The decoder icon toggles to a debug button.

The following functions are available in the decoder window

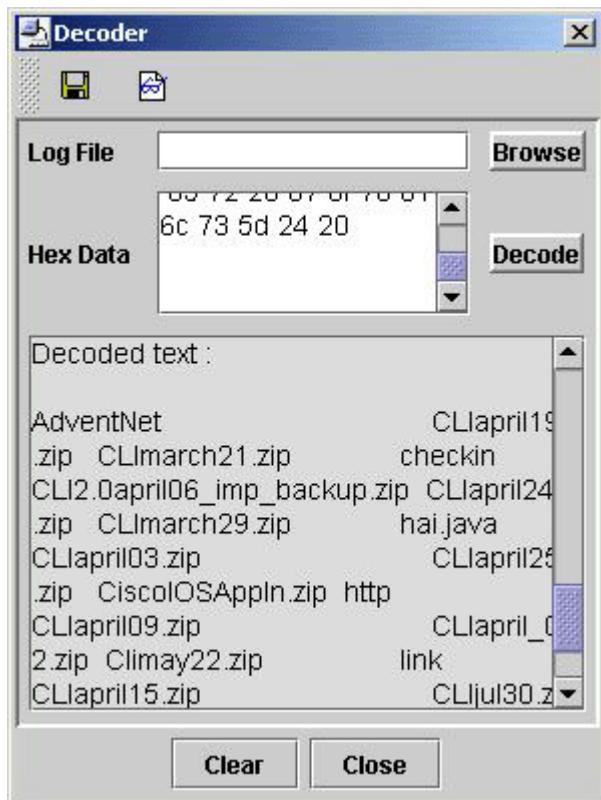
- Save CLI Browser decoder results - Saves the debug information to a file.
- Debug - switches to the debug window.

## Performing the Decoding Operation

The CLI decoder is used to decode the CLI debug messages. The decoding can be done in two ways by using the following options.

- Copy-Paste option
- File option

The figure below depicts the CLI Decoder.



### Copy-Paste Option

This option can be used for frequent debugging.

- Copy the debug information in the debug window.
- Click the CLI decoder icon, this will switch to the decoder window.
- Paste the debug message into the "Hex PDU" text area.
- Click the Decode button.

The decoded message is displayed in the bottom panel of the Decoder window.

### File Option

This option can be used if the debug message was stored in a file and decoding has to be done.

Load the file that contains the debug information and click the Browse button in the Debug Window. You can also enter the URL in the File URL text field and press the "ENTER" key.

This will display the decoded message in the bottom panel of the Decoder Window.

## 6.15.3.10 Command Generation

---

- Command Structure
  - Command Set
  - Data Set
- 

### Command Structure

Command generation now become easier with XML based Command Set and Data Set. The commands can be configured in CLI Browser to have a list of commands in the CLI tree.

The Command Set has a list of command templates. Each command template represents a particular CLI command for a specific device. The command can be generally represented as follows:

```
<command> <object> <parameters> <options> <help>
```

Where,

**<command>** : is the name of the command. For example in UNIX OS, listing the directory **<command>** can take the value '**ls**'. Following are a few examples of various commands that are used in a UNIX system:

- netstat
- who
- pwd

**<object>**: represents the object on which the command takes effect. In UNIX OS for the command 'ls', the value of the object can be the directory for which the contents are to be listed. Objects in turn can have sub objects, which can have more sub-objects and so on. The following are a few examples on a UNIX system.

- Directory name for an 'ls' command.
- eth0 (Ethernet interface for which the statistics is required for the netstat command)
- User name or group name for user/group management commands.

**<parameters>**: represents the parameters for the command. The parameters can also occur in the form **<parameter name>=<value>** in certain commands.

**<options>** :it could be the various options that the command can accept and configuration parameters.

The following are some examples:

- -l for the 'ls' command (long listing)
- -u for displaying the udp statistics for a netstat command

### Command Set

Command Set is used to define a set of XML based command templates for a particular device. All the possible commands (configuration, monitoring commands, etc.) for a particular device can be included in this file.

The Command Set contains the command template (**commandset.dtd**) or structure (syntax) of the command that is available in <Web NMS Home>ccs directory. The table given below is a list of parameters grouped under the COMMAND-SET tag, with a brief description.

| Tag                     | Description                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>STR-COMMAND-LIST</b> | It includes a list of commands in a command set file.                                                                                                                                                                                                                                                                                                                     |
| <b>COMMAND</b>          | Represents the actual command and contains following attributes:<br>1. NAME: identifies the command.<br>2. DELIMITER: The delimiter to be used between two objects.                                                                                                                                                                                                       |
| <b>OBJECT</b>           | Represents a single command template or structure that contains following attributes to identify the object:<br>1. NAME: The object name.<br>2. DELIMITER: The delimiter between succeeding elements.<br>3. DESCRIPTION: It contains the meaning of the object.                                                                                                           |
| <b>PARAM</b>            | Represents the actual parameter format that contains following attributes to identify the param:<br>1. NAME : The parameter name<br>2. PARAMTYPE: It may be either VALUE type or NAMEVALUE.<br>3. VALUETYPE: It may be int, char, float, or string type.<br>4. OPTION_FLAG: It may be MANDATORY or OPTIONAL.<br>5. DESCRIPTION: It contains the meaning of the parameter. |
| <b>OPTIONS</b>          | To denote the various options that command can append. It contains the following elements :<br>1. SIMPLE_OPTS: simple option without arguments.<br>2. SIMPLE_OPT_ARGS: simple option with arguments.<br>3. LONG_OPTS: long option without arguments.<br>4. LONG_OPT_ARGS: long option with arguments.                                                                     |
| <b>HELP</b>             | To provide help to a command.                                                                                                                                                                                                                                                                                                                                             |

The following examples illustrate the forming of a command set.

1. Listing a directory in UNIX operating systems.
2. Show Command to get the details of CISCO devices.

### Example1: Listing a Directory in UNIX Operating Systems.

```

<COMMAND NAME="ls" DELIMITER=" " >
<OPTIONS DESCRIPTION="Options to list contents of directory " >
<SIMPLE_OPTS OPT_PREFIX="-" />
<SIMPLE_OPTS OPT_PREFIX="--" />
<SIMPLE_OPTS OPT_PREFIX="--" />
<SIMPLE_OPTS OPT_PREFIX="--" />
<LONG_OPT_ARGS OPT_NAME="time" TYPE="char" OPT_DEP="" 
OPT_PREFIX="--" />
</OPTIONS>
<HELP>
<DESCRIPTION>List the contents of directories.</DESCRIPTION>
</HELP>
</COMMAND>
```

The above example command template is defined for listing directories on UNIX systems. It contains the command name **ls** and different simple options. The option contains only the prefix for options.

Refer to **unixcmds.ccs** file available in <Web NMS Home>/ccs directory.

### Example2: Show Command to Display the Details of CISCO Devices

```
<COMMAND NAME="show" DELIMITER=" " >
<OBJECT NAME="ip" DESCRIPTION=" " >
<OBJECT NAME="access-list" DESCRIPTION=" " >
<OBJECT NAME="compiled" DESCRIPTION=" " />
<PARAM NAME="access-list-number" PARAMTYPE="VALUE"
VALUETYPE="INT" DESCRIPTION=" " />
<PARAM NAME="name" PARAMTYPE="VALUE" VALUETYPE="CHAR"
DESCRIPTION=" " />
</OBJECT>
</OBJECT>
</COMMAND>
```

The above example command template is defined to send **show** commands to display detailed system and protocol information of CISCO devices.

Refer to **showcmds.ccs** file available in <Web NMS Home>/ccs directory.

### Data Set

For each Command Set, there will be an associated Data Set, which contains all the data definitions needed for the corresponding commands. These data definitions are in the form of an XML with file extension **dat**.

The Data Set (**dataset.dtd**), which contains instances of the commands in the Command Set is available in <Web NMS Home>/ccs directory.

The table given below is a list of parameters grouped under the DATA-SET tag, with a brief description.

Tag	Description
<b>STR-DATA-SET</b>	It includes a list of data values in a data set file.
<b>CMDATA</b>	It includes a list of commands in a command set file. It contains the NAME attribute for identifying the command in the command set to which the data belongs.
<b>DATA</b>	It has a list of data instances for a particular command.
<b>OBJECT</b>	It is similar to that in the Command Set except that it represents the value (data) for the object. It has a NAME attribute to identify the object.
<b>PARAM</b>	It contains all the values of the parameters in the command. It has the following attributes: <ol style="list-style-type: none"> <li>NAME: the name of the parameter.</li> <li>VALUE: indicates that it contains only the value.</li> </ol>
<b>OPTIONS</b>	It denotes the various options that command can append. It contains the following elements : <ol style="list-style-type: none"> <li>SIMPLE_OPTS: simple option without arguments.</li> <li>SIMPLE_OPT_ARGS: simple option with arguments.</li> <li>LONG_OPTS: long option without arguments.</li> <li>LONG_OPT_ARGS: long option with arguments.</li> </ol>

The following examples illustrate the usage of forming a Data Set corresponding to a Command Set.

1. Listing a directory in UNIX operating systems.
2. Show Command to get the details of CISCO devices.

## Example1: Listing a Directory in UNIX Operating Systems.

```
<CMDDATA CMDNAME="ls">
<DATA NAME="ls">
<OPTIONS>
<SIMPLE_OPTS OPT_VAL="l" />
<SIMPLE_OPTS OPT_VAL="a" />
<SIMPLE_OPTS OPT_VAL="d" />
<SIMPLE_OPTS OPT_VAL="f" />
<LONG_OPT_ARGS OPT_NAME="time" OPT_ARG="status" />
</OPTIONS>
</DATA>
</CMDDATA>
```

The above example command template is defined for listing directories on UNIX systems. It contains the actual command name **ls** with different simple options that have to be sent to the device. The above data instance is for the command **ls** in UNIX systems. With the long listing format, it can be noticed that the above definition contains only data for the previously defined command template and it is almost similar to the command template.

Refer to **unixcmds.dat** file available in <*Web NMS Home*>/ccs directory for complete details.

## Example2: Show Command to Get the Details of CISCO Devices.

```
<CMDDATA CMDNAME="show">
<DATA NAME="dataname">
<OBJECT NAME="ip" VALUE="ip">
<OBJECT NAME="access-list" VALUE="access-list">
<OBJECT NAME="compiled" VALUE="compiled"/>
<PARAM NAME="access-list-number" VALUE="101"/>
<PARAM NAME="name" VALUE="name"/>
</OBJECT>
</OBJECT>
</DATA>
</CMDDATA>
```

The above example command template is defined to send the actual **show** commands to devices to display detailed system and protocol information of CISCO devices. The command consists of an object, which has parameters that have to be sent to the device.

Please refer to **showcmds.dat** file available in <*Web NMS Home*>/ccs directory for complete details.

### 6.15.3.11 Internationalization

AdventNet CLI Browser supports Internationalization. This allows using the CLI Browser application in various languages without changing the source code. Localized content can be added easily and the same executable can be run worldwide. All the textual elements such as GUI component labels, and messages can be made suitable to the locale (combination of specific language and country) of the user.

The following are the steps involved in enabling the Internationalization support to AdventNet CLI Browser.

1. The **CLIBrowser.properties** file available in the <Web NMS Home>/html directory is to be used as the template file. This file contains the English strings of all the GUI labels and the messages.
2. The CLIBrowser.properties file has to be copied to the specified locale file. For example, to display the CLIBrowser in French language, the CLIBrowser.properties file is to be copied as CLIBrowser\_fr\_FR.properties file. The language and the country are to be represented by the standard two-letter codes (fr - French and FR - France). If the specified locale file is not present in the specified directory, the default properties file CLIBrowser.properties is searched and loaded.
3. The developer has to write the equivalent strings of the chosen language and country in this file. This will enable the CLIBrowser to print the user-written strings instead of English strings. For all the strings for which corresponding locale-specific strings are not given, English strings are used.



**Note:** The format given in the CLIBrowser.properties file should not be altered. The english strings are provided with the escape sequence characters. For example, the string "Save CLIBrowser Results As...." is provided as "Save\ CLIBrowser\ Results\ As...". However, the equivalent strings (of the chosen language) need not have the "escape" sequence included. For example, the equivalent string for "Save\ CLIBrowser\ Results\ As... ". can be given as "my own language equivalent of the same text".

4. After creating CLIBrowser.properties file for the language to be localized, invoke the **CLIBrowser.bat/sh** file available in the <Web NMS Home>/bin/browsers directory as given below:

```
CLIBrowser.bat/sh -i -L en,US -S conf
```

Where,

- i is internationalize
- L is locale (This includes language and country separated by comma)
- S is filepath (The path where the .properties file is present)

## Appendix

---

- A: Discovery
  - B: Fault
  - C: Performance
-

## Appendix A: Discovery

- 
- Add Node
  - Add Network
  - TL1 Protocol Properties
- 

### Add Node

This section explains the fields in the Add Node dialog box.

- SNMP Node
- TL1 Node
- CORBA Node

#### SNMP Node

By default, all IPv4 devices are discovered and hence the **IPv4** option is selected. If you need to discover an IPv6 node in the network, select the **IPv6** radio button and specify appropriate values for the remaining fields. Only the fields (as explained in the table given below) with an asterisk \* are applicable when you select IPv6.

Field	Description
IPAddress / Host Name*	Specify the IP address or name of the device to be discovered.
Netmask	Specify the netmask. By default, the value is <b>255.255.255.0</b> .
Discover even if node is not reachable?*	If this option is checked, even if the node is not alive when you add it, Web NMS adds a managed element for that node.
Discover all devices in parent network?	If this option is selected, apart from adding the node that you have configured, all other devices in their parent network are also discovered (if they were not discovered already).  For example, if you add a device 192.168.1.5 with this option checked, then all the devices in the 192.168.1.0 network are also discovered.  If this option is not selected, then the device is added and the corresponding parent network is also added (if they were not added already) to the database. But there will not be any discovery for this network.
Override Seed.file filters ?*	Initially some configurations are made related to discovery in the seed.file using Discovery Configurator tool. A configuration could have been made to

Field	Description
	restrict the discovery of certain nodes. But if you select this option, those configurations are overridden and discovery is performed for those nodes also.
Update configurations in Seed.file ?*	Select this option if you want this node to be discovered the next time the Web NMS Server is started (after reinitializing). On doing so, the node that you mention is configured in the seed.file permanently.
Community*	By default, the value is <b>public</b> . When no value is set, then the community value as configured in the <b>seed.file</b> is fetched and substituted.
Process Add Node request in the background*	Once the <b>Add Node</b> operation is committed, Web NMS takes a while to discover the network and its elements. If you do not want to wait for the discovery to be completed and want to proceed with other operations, select this option. By doing so, you can quit the current view and work on other views while the discovery process is done in the background.
Snmp Agent Port*	Port number where the SNMP agent is running. By default, the port is <b>161</b> .
SNMPv3 Enabled ?*	If you enable the discovery of SNMPv3 devices, then you need to specify the user name and context name in the corresponding fields.
User Name*	
Context Name*	

The following table gives a few combination of configurations made in the SNMP Add Node dialog box and its outcome.

Field	Description
<b>IPAddress / Host Name:</b> 192.168.10.210	<b>Immediate Effect</b> - The device/node and the network are added. Immediate discovery of the parent network (of the node added) is also done.
<b>Discover all devices in parent network?:</b> Enabled (ticked)	<b>Warm Start</b> - The node and the network are added. Immediate discovery of the parent network (of the node added) is also done.
<b>Update configurations in Seed.file ?:</b> Enabled (ticked)	<b>Cold Start</b> - Neither the node nor the network gets added and the discovery of the network is also not carried out (since discovery itself is disabled).
<b>IPAddress / Host Name:</b> 192.168.10.210	<b>Immediate Effect</b> - The node and the network are added. But, parent network discovery (of the node added) is not carried out

Field	Description
<b>Discover all devices in parent network?:</b> Disabled (not ticked)  <b>Update configurations in Seed.file ?:</b> Disabled (not ticked)	<p><b>Warm Start</b> - The node and the network are added. But, the parent network discovery (of the node added) is not carried out (but the already discovered entries of the network if any, persists in the database).</p> <p><b>Cold Start</b> - The node and the network are added. Immediate discovery of the parent network (of the node added) is also done.</p>
<b>Node:</b> 192.168.10.210  <b>Discover all devices in parent network?:</b> Enabled (ticked)  <b>Update configurations in Seed.file ?:</b> Disabled (not ticked)	<p><b>Immediate Effect</b> - The node and the network are added. Immediate discovery of the parent network (of the node added) is also done.</p> <p><b>Warm Start</b> - The node and the network are added. Immediate discovery of the parent network (of the node added) is also done.</p> <p><b>Cold Start</b> - The node and the network are added. But parent network discovery of the node added is not carried out.</p>

## TL1 Node

Field	Description
Node*	
Netmask	
Community*	
Override Seed.file filters ?	Refer to the field description in Adding an SNMP Node.
Discover even if node is not reachable?*	
Discover all devices in parent network?	
Process Add Node request in the background*	
TL1 Device Group Name*	Select the group name to which the node had to be added from this drop-down box.

## CORBA Node

Field	Description
<b>CORBA Properties</b>	
ORB Host Name / IPAddress	The name or IP address of the host in which the tnameserver is running. <b>Example:</b> localhost
ORBPort	The port number in which the tnameserver is listening. <b>Example:</b> 1050
Name Reference	The name with which the agent has registered itself in the name service (tnameserver) for its communication. <b>Example:</b> 192.168.5.105

Field	Description
Interface Name	The name of the interface that the agent has implemented for its communication. <b>Example:</b> ADSL.ADSLLine
ORB Class Name	The fully qualified class name of the ORB implementation class to be used (for example, Java IDL provides a default implementation for the fully functional ORB which needs to be specified as <b><i>com.sun.corba.se.internal.iop.ORB</i></b> ). Support for OpenORB and Orbix have been introduced in addition to default Java IDL implementation.
Managed Object Properties	
Group Name	The name of the Group to which the CORBA node belongs. <b>Example:</b> ADSL
Type	The name for a type under which the added node can be classified. By default, only CORBA nodes whose type is <b>corba_node</b> are displayed.
User Tester class for Status Polling	The class to be used for status polling. The default class <b><i>com.adventnet.nms.topodb.CORBAStatusPoller</i></b> can be used if the status poll operation (method) does not have any arguments and returns an int as severity as described in STATUS POLL COMMAND.
Command for Status Polling	
Interface Name	The name of the interface that the agent has implemented for status polling. <b>Example:</b> ADSL.ADSLLine
Name Reference	The name with which the agent has registered itself in the name service (tnameserver) for status polling. <b>Example:</b> 192.168.5.105
Operation Name	The method name to be used for the status polling. This method should not take any parameter and should return only an integer. <b>Example:</b> getLineStatus
Object for Data Collection	
Interface Name	The name of the interface that the agent has implemented for data polling. <b>Example:</b> ADSL.ADSLLine
Name Reference	The name with which the agent has registered itself in the name service (tnameserver) for data polling. <b>Example:</b> 192.168.5.105
Process Add Node request in the background	Refer to the field description in Adding an SNMP Node.

## Add Network

This section explains the fields in the Add Network dialog box.

Field	Description
Network Address	Specify the IP address of the network to be discovered.
Netmask	Specify the netmask. By default, the value is <b>255.255.255.0</b> .
Managed	If this option is selected, the network is added to the database and discovery happens. The network and its elements are in managed state as they are discovered.  If this option is not selected, the network is added in unmanaged state to the database and discovery of that network will not be started. Hence none of the network elements in the network will be discovered.
Start Discovery	If this option is selected, the discovery of the added network starts instantly.  If the option is not selected, then the network is just added to the database but discovery of that network is not performed.
Add Overriding The Seed File Configuration?	Initially some configurations are made related to discovery in the seed.file using Discovery Configurator tool. A configuration could have been made to restrict the discovery of certain nodes. But if you select this option, those configurations are overridden and discovery is performed for those nodes also.
Return Immediately After Submitting Request?	Once the <b>Add Node</b> operation is committed, Web NMS takes a while to discover the network and its elements. If you do not want to wait for the discovery to be completed and want to proceed with other operations, select this option. By doing so, you can quit the current view and work on other views while the discovery process is done in the background.
Write To Seed File	Select this option, if you want this node to be discovered the next time the Web NMS Server is started (after reinitializing). On doing so, the node that you mention is configured in the seed.file permanently.

## Dependency between 'Managed' and 'Start Discovery' options

**Managed** - enabled (ticked)  
**Start Discovery** - disabled (not ticked)

In this case, the network will be added and will be managed. But, discovery for the network will not happen. However, status polling will take place.

**Managed** - unchecked  
**Start Discovery** - checked

In this case, the network will be added, but will be unmanaged. This means, discovery or status polling will not happen for this network (even though Start Discovery option is checked).

## TL1 Protocol Properties

This section explains the fields in TL1 Protocol Properties of the Discovery Configurator.

Option [MO]	Description
<b>Device Group</b> [deviceGroupName]	<p>Specify the name of each device group.</p> <p>This is used to provide runtime addition of TL1 devices in Web NMS. Once you have configured all the necessary parameters at the device group level and specified a device group name, you can use the runtime Add Node facility from the Web NMS Client to discover and add any TL1 device that you may have forgotten to configure in the tl1seed.file. When you do this runtime addition of TL1 devices, you need to choose the device group to which the TL1 device belongs in the Add Node user interface of the Web NMS Client. All parameters specified for that device group will be used to discover, connect, and add the TL1 Managed Objects to the topology database.</p>
<b>Type</b> [type]	<p>This denotes the type of TL1 device which need to be discovered. Each type of TL1 device can be differentiated by specifying different values for the type field. This type field is stored in the Managed Object type field used by Web NMS to differentiate different types of devices and provide Multiple Device Support. This field is required since different types of TL1 devices have different command sets, connection handlers, etc. The default type value is TL1Node.</p>
<b>Port</b> [tl1port]	<p>This denotes the port in which the TL1Agent is running. The port needs to be specifically given, since the TL1 Agent is not running on any specific port.</p>
<b>Status Poller</b> [statpoll_command]	<p>You can set up status polling commands for devices by specifying one or two commands as statpollCommand. Optionally, you can specify the contents of successful or clear response in the response field. The status polling commands and the response content provided will be used to poll the status of the TL1Interface ManagedObject, interpret the TL1 Response Messages, and allocate appropriate severity to the device.</p> <p>Based on the status polling information specified in the tl1seed.file, Web NMS does the status polling and allocates severity based on a generic status polling logic. But occasionally as a user or administrator, you may want to implement a more specific status polling logic for certain TL1 devices. For this purpose, you can write your own status poller usertester class to do the status polling and allocate appropriate severity depending upon the response messages. This status poller usertester class can be set up for any device in the tl1seed.file itself by making a uClass entry. For more detailed information on status polling logic and how to write status pollers, refer to the <b>README.html</b> file under the &lt;Web NMS Home&gt;/default_impl/tl1_impl/status_polling directory.</p>

Option [MO]	Description
	Response parameters, if specified for a statpollCommand, will be used for deciding the severity of the device by comparing the Response Message parameters obtained from the device with the response field information specified.
<b>Connection Handler</b> [Connection Handler]	This denotes the Connection Handler class which needs to be used for establishing a TL1 session with a TL1 device. You need to specify the appropriate or blank connection handler for the respective type of TL1 device. For more information, refer to Connection Handler.
<b>AppendFront</b>	A string (specific to a TL1 device) to be prefixed to every TL1 message, can be configured using this option.
<b>AppendEnd</b>	A string (specific to a TL1 device) to be prefixed to every TL1 message, can be configured using this option.
<b>Login</b> [login_command]	The TL1 device needs a login command to communicate. Ensure that you specify the correct login command against the loginCommand parameter. This login command will most probably correspond to a particular user, with password. Web NMS server uses this command to open a session with the TL1 device as part of discovery and uses this session for all subsequent communication with the device. That is, it's equivalent to Web NMS login and communicating with the TL1 device as the specific user given in the login command.
<b>Init</b> [init_command]	<p>You can also specify other commands as part of discovery. Maximum of two commands that are to be used for specific initialization of the TL1 device can be specified as initCommand. The init command is meant for clearing the memory, error counts, preexisting data, etc., in the device. This command is meant for initializing the TL1 device. The login and init commands will be sent to the device every time a TL1 session is opened by Web NMS, i.e., both during Web NMS Cold Start and Warm Start.</p> <p>parameters="GATEWAYSTATE=GATEWAY,GATEWAYIP=IP,"</p> <p>The GATEWAYSTATE field in the response message is mapped to the GATEWAY property of the managed object, and the GATEWAYIP field in the response message is mapped to the IP property of the managed object. You can customize this command and retrieve the fields in the response message and map it to the managed object property as per requirement.</p>
<b>Info</b> [info_command]	<p>The info command is meant for retrieving more information about the TL1 device, which can be used to store as managed object properties. Basically, this command is used for collection of device data immediately after discovery. This set of commands will not be used on Warm Start of Web NMS. Because, these properties are unlikely to change during rediscovery of the object. These info commands are sent to the device only once during Cold Start.</p> <p>parameters="GATEWAYIPMASK=MASK,GATEWAYBRDCASTIP=BRDCAST,"</p> <p>The GATEWAYIPMASK field in the response message is mapped to the MASK property of the managed object and the GATEWAYBRDCASTIP field in the response message is mapped to the BRDCAST property of the managed object. You can customize this command and retrieve the fields in the response message and map it to the managed object property as per requirement.</p> <p>The init command is different from the info command. The init command is meant for initializing the device, whereas the info command is meant for retrieving the values of the parameters for storing as TL1 object properties immediately after discovery.</p>

Option [MO]	Description		
	<p><b>Note:</b> For <i>loginCommand</i>, <i>initCommand</i>, and <i>infoCommand</i>, you can specify response message parameters that need to be used. All the response parameters specified against the above three messages will be extracted from the response messages and stored as ManagedObject properties.</p> <p>In the example entries, configured <i>response="GATEWAYSTATE=GATEWAY,..."</i> means that the GATEWAY parameter will be extracted out of the TL1 response message and stored in the ManagedObject under the property name GATEWAYSTATE. If you specify it as <i>response="GATEWAY,..."</i> then the GATEWAY parameter will be extracted and stored in the same name.</p> <p>These commands are typically commands meant for collecting certain information at the whole device/system level, i.e., there will be only one instance of each parameter. But if there are multiple instances of the same parameter in the Response Message, say corresponding to multiple sub-components (e.g., cards, ports, etc.), values corresponding to the first instance of the parameters will be collected. Also, as of now, data can be collected for only parameters which are name-value pairs. Position-defined parameters are ignored. But as such, this facility should suffice for almost all situations.</p> <p>This content upgrade usually happens when Web NMS connects to the device for the first time during discovery. But if that failed due to some reasons such as the TL1 Agent being down, you can solve the problem in the device and open Web NMS Client and do a reconnect to the TL1 device using the <b>Connect Device</b> menu item available in the TL1Menu. Content upgrade will automatically happen at this time.</p>		
<b>Status</b>	<p>This configuration monitors the status of the devices.</p> <p>Response message for the status command can be configured using this option.</p> <table border="1" data-bbox="461 1529 1431 2030"> <tr> <td data-bbox="461 1529 588 2030"></td><td data-bbox="588 1529 1431 2030"> <p><b>Warning:</b></p> <ul style="list-style-type: none"> <li>• Some special characters are interpreted differently by the database drivers. Also, some special characters are internally used by Web NMS to store these commands and response information and to retrieve them from the database as hashtable for ease of use. Take care not to use the following special characters in the parameters: #, {, }, &lt;, &gt;</li> <li>• This provision for specifying device discovery commands is meant only for most essential commands. Take care to specify only one or two commands as there is a limitation in the column size in the database. If you really need to increase this size then you need to modify the column size accordingly in the Database_Schema file for TL1Node and TL1Interface tables.</li> </ul> </td></tr> </table>		<p><b>Warning:</b></p> <ul style="list-style-type: none"> <li>• Some special characters are interpreted differently by the database drivers. Also, some special characters are internally used by Web NMS to store these commands and response information and to retrieve them from the database as hashtable for ease of use. Take care not to use the following special characters in the parameters: #, {, }, &lt;, &gt;</li> <li>• This provision for specifying device discovery commands is meant only for most essential commands. Take care to specify only one or two commands as there is a limitation in the column size in the database. If you really need to increase this size then you need to modify the column size accordingly in the Database_Schema file for TL1Node and TL1Interface tables.</li> </ul>
	<p><b>Warning:</b></p> <ul style="list-style-type: none"> <li>• Some special characters are interpreted differently by the database drivers. Also, some special characters are internally used by Web NMS to store these commands and response information and to retrieve them from the database as hashtable for ease of use. Take care not to use the following special characters in the parameters: #, {, }, &lt;, &gt;</li> <li>• This provision for specifying device discovery commands is meant only for most essential commands. Take care to specify only one or two commands as there is a limitation in the column size in the database. If you really need to increase this size then you need to modify the column size accordingly in the Database_Schema file for TL1Node and TL1Interface tables.</li> </ul>		

## Appendix B: Fault

- Configuring Trap Parsers
- Trap Protocol Data Unit Information
- Event Properties
- Alarm Properties

### Configuring Trap Parsers

The following table explains each of the fields in **Trap Parser Configuration** tool..

Field	Description
Trap Port	<p>Identifies the port number to which to listen for traps.</p> <p>The trap port is the port at which the Web NMS server listens for SNMP notifications.</p> <ol style="list-style-type: none"> <li>1. The specified Port(s) is not associated with a particular Trap Parser, but a general configuration.</li> <li>2. When no port has been specified, traps will not be received at all.</li> <li>3. Multiple ports can be specified using a comma separator, for example - 8001,8002</li> <li>4. The default configuration for Trap Port (listed in the Trap Port field) will be the port(s) specified in <i>&lt;Web NMS Home&gt;/conf/trapports.conf</i></li> <li>5. Ensure that the specified ports are free.</li> </ol>
Name	Name to identify the parser.
Match Criteria	Determines the traps that are parsed by the Trap Parser to generate an event.
Nodes	<p>Match criteria based on the source of the received trap matching one of the specified nodes listed in the field.</p> <ol style="list-style-type: none"> <li>1. This is an optional match criterion.</li> <li>2. For an SNMPv1 trap, the agent address returned by the trap is used when matching the property value. For SNMPv2c, the source address returned by the trap is used when matching the property value.</li> <li>3. Use the comma separator to specify more than one node. <b>Example:</b> printer2,printer4</li> <li>4. You can use Wildcard (*) and Negation (!) characters in this field.</li> </ol>
Groups	<p>Match criteria based on the source of the received trap that belongs to one of the groups specified. (Web NMS provides a way to group a set of MOs based on some of their characteristics.)</p> <ol style="list-style-type: none"> <li>1. This is an optional match criterion.</li> <li>2. Use the comma separator to specify more than one group. <b>Example:</b> groupX,groupY</li> <li>3. Do not use Negation (!) or Wildcard (*) characters in this field</li> </ol>
Enterprise	Associated with the SNMP V1 button only.

	<p>Specify the enterprise object ID (OID) of the SNMPv1 trap. When specified, the parser is applied only if the incoming trap's enterprise OID starts with what is specified in this field.</p> <p>If the enterprise OID is specified as .1.3.6.1.2.1.11, all the OIDs under this tree are matched for traps. To avoid this kind of matching, enter the enterprise OID value in angular brackets, such as &lt;.1.3.6.1.2.1.11&gt;</p> <p>If the value is given as “*”, then all the OIDs are matched.</p>
Generic Type	<p>Associated with the SNMP V1 button only.</p> <p>Each SNMPv1 trap has a generic type number which can be specified as a match criterion. When specified, the Trap Parser is applied only if the incoming traps match the specified generic type number.</p>
Specific Type	<p>Associated with the SNMP V1 button only.</p> <p>Each SNMPv1 trap has a specific type number which can be specified as a match criterion. When specified, the Trap Parser is applied only if the incoming traps match the specific type number.</p>
Trap OID	<p>This field is available only when you click the <b>Click here to configure for V2C &amp; V3</b> button.</p> <p>An SNMP V2C or SNMP V3 trap is uniquely identified by Trap OID that is associated with the Trap Protocol Data Unit (PDU). This trap OID can be specified as a match criterion.</p> <ol style="list-style-type: none"> <li>1. The Trap Parser is applied only if the incoming trap has a value that starts with the OID specified in this field.</li> <li>2. When a trap OID is specified, all traps that start this OID are matched and the Trap Parser is applied. If you want to match the exact OID, specify the trap OID within angular brackets &lt;&gt;.</li> <li>3. Wildcard - Asterix(*) character can be used.</li> </ol>
Severity	<p>Indicates the state of the event that determines the severity shown in the Event Viewer.</p> <p>This severity determines how an alarm is affected by this event. For a given failure object, the severity specified for the event correlates with the severity of the corresponding alarm.</p>
Message	Corresponds to the text field of the event object. The value specified here is entered in the text field of the event object created by this Trap parser.
Failure Object	Appropriate processing by the Trap parser ensures that the failure object reflects the exact problem. This is used to quickly track problems and identify the objects instead of simply reporting raw events.
Domain	Use to specify the domain name of an event. This field is optional.
Category	Use to categorize events and alarms.
Network	Identifies the network name from which the event has occurred. This field is optional.
Node	The node value of the event. This field is optional.
Source	Identifies the source name of an event. If the status of the MO is updated with the severity of the event, then the source should match the name of the MO, which should be updated. Identification of the source is the only way in which the status of the MO can be updated in the Web NMS server.
Group Name	Enables you to group meaningful events.
Help URL	The URL (absolute or relative to the <Web NMS Home> directory) that can be configured to provide detailed help for a given event..

## Trap Protocol Data Unit Information

**Important:** To specify Trap PDU information for **Trap Parser** fields, use the **dollar (\$)** notation. For **Event Parsers** and **Event Filters**, use **percentage (%)** notation instead of dollar (\$). The @ notation remains the same for all the three configurations.

Field	Description
\$Agent	<p>SNMP V1 Traps</p> <p>If the device corresponding to the agent address returned by the trap has been discovered by Web NMS, this token fetches the name of the parent managed object (MO) corresponding to the interface object matching the agent address of the trap received.</p> <p>If the device corresponding to the agent address of the trap has not been discovered, this token returns the corresponding IP address of the agent address from which the trap has been received.</p> <p>For example, a trap is received from an agent and the corresponding device has been discovered by Web NMS with the interface object of 'IF-webserver' and the name of the parent managed object is 'webserver'. In this scenario, %Agent returns webserver. If the device is not yet discovered, %Agent returns the IP address, such as 192.168.1.30.</p> <p>SNMP V2C &amp; V3 Traps</p> <p>If the device corresponding to the source address contained by the received trap has already been discovered by Web NMS, this token fetches the name of the parent MO that corresponds to the interface object matching the source address of the received trap. If the device corresponding to the source address of the trap has not been discovered, this token returns the IP address of the source of the trap.</p>
\$Community	This token is replaced by the community string of the received trap.
\$Enterprise	This token is replaced by the enterprise ID of the received trap. This token is applicable to SNMP traps only, for non-SNMP traps it is replaced with “”.
\$GenericType	This token is replaced by the generic type of the received trap. This token is applicable to SNMP V1 traps only. For non-SNMP traps, it is replaced with “”.
\$Source	If the device corresponding to the source address contained by the received trap has been discovered by Web NMS, this token fetches the name of the parent MO that corresponds to the interface object matching the source address of the received trap. If the device corresponding to the source address of the received trap has not been discovered, the corresponding IP address of the source address is returned.
\$SpecificType	This token is replaced by the specific type of the received trap and is applicable to SNMP v1 traps only. For non-SNMP traps, it is replaced with “”.
\$Uptime	This token is replaced by the up-time value in the received trap.
\$TrapOID	This token is replaced by the trap OID of the received trap. This token is applicable to SNMP V2C traps only. For non-SNMP traps, it is replaced with “”.

Field	Description
\$*	This token is replaced by all the variable bindings (both OID and variable values) of the received trap.  Example: For the following varbinds, 2.2.1.1.221 INTEGER 30 .1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10The result is ifIndex: 30, sysDescr: abc, ifIndex: 10
\$#	This token is replaced by all the variable binding values (only variable values and not OIDs) of the received trap.  Example: For the following varbinds, 2.2.1.1.221 INTEGER 30 .1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10  The result is 30, abc, 10
\$N	For this token, N is a non-negative integer. This token is replaced by the (N+1)th SNMP variable value in the variable bindings of the received trap. The Index N starts from 0.  Example: For the following varbinds, 2.2.1.1.221 INTEGER 30 .1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10  For %1, the result is abc
@*	This token is replaced by all the OID labels in the variable bindings of the received trap.  Example: For the following varbinds, 2.2.1.1.221 INTEGER 30 .1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10  The result is ifIndex: sysDescr: ifIndex
@N	This token is replaced by the (N+1)th OID value in the variable bindings of the received trap. The index count starts from 0. This token is replaced by the (N+1)th OID label in the variable bindings of the received trap. The index starts from 0.  Example: For the following varbinds, 2.2.1.1.221 INTEGER 30 .1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10  For @1, the result is sysDescr
\$IP-Source	This token is replaced by the IP address corresponding to the source address of the received trap.
\$IP-Agent	This token is replaced by the IP address corresponding to the agent address of the received trap.
Special Purpose Tokens	Note: The associated Managed object should have been discovered already by Web NMS for using the following special purpose tags (or tokens). This is applicable to all special purpose tags (or tokens) enumerated in this section.
\$AgentMO	This token enables access to managed object properties. The tag can be used to access any properties of the parent managed object for the interface object corresponding to the agent address of the received trap. (Fetching the MO is similar to the \$Agent tag mechanism). For example, if you want to access the pollInterval property of the parent MO that corresponds to the agent address of the received trap and assign it to some property of the generated

Field	Description
	<p>Event object, you must specify the tag as \$AgentMO(pollInterval) against the specific property of the event.</p> <p>Usage: \$AgentMO(PropertyName)</p>
\$IF-AgentMO	<p>This token is similar to \$AgentMO, except that the properties of the interface MO that corresponds to the agent address of the received trap can be accessed using this tag. In the case of SNMP V2C traps, it is exactly the same as \$IF-SourceMO.</p> <p>Usage: \$IF-AgentMO(PropertyName)</p>
\$IF-Agent	<p>This token is similar to \$Agent, except that it results in the interface MO name that corresponds to the agent address of the trap received. In the case of SNMP V2C traps, it is exactly the same as \$IF-Source.</p> <p>Usage: \$IF-Agent</p>
\$SourceMO	<p>This token can be used to access any properties of the parent MO for the interface object that corresponds to the source address of the received trap. (Fetching the MO is similar to the \$Source tag). For example, if you want to access the pollInterval property of the parent managed object corresponding to the source address of the received trap and assign it to some property of the event, you must specify the tag as \$SourceMO(pollInterval) against the specific property of the event.</p> <p>Usage: \$SourceMO(PropertyName)</p>
\$IF-SourceMO	<p>This token is similar to \$SourceMO, except that the properties of the interface MO that corresponds to the source address of the received trap can be accessed using this tag.</p> <p>Usage: \$IF-SourceMO(PropertyName)</p>
\$IF-Source	<p>This token is similar to \$Source, except that it results in the interface object name that corresponds to the source address of the received trap.</p> <p>Usage: \$IF-Source</p>

## Event Properties

S.No.	Name	Replaceable Parameter (Property Token)	Description
1.	<b>severity</b>	\$severity	<p>The present severity value (e.g., 1, 2, etc.) of the event.</p> <p>Severity values set for an Event are provided in <b>SeverityInfo.conf</b> present in the &lt;Web NMS Home&gt;/conf directory.</p>
2	<b>text</b>	\$text	<p>Holds the description of the fault.</p> <p><b>Example:</b> If the event is for a fault indicating high processor load then the text can be set as <b>Processor load high</b>.</p>
3	<b>entity</b>	\$entity	<p>Represents the failure object.</p> <p>Value of entity is closely coupled with the way you model your network element.</p> <p><b>Example:</b> Consider a network element as a user's PC. You model User's PC as a ManagedObject. It can have failure objects, such as CPU, Keyboard, Monitor, etc.</p> <p>As per the above modeling, event which is generated from user's PC, can have entity, such as CPU, Keyboard, or Monitor.</p>
4	<b>source</b>	\$source	<p>Represents the source of failure.</p> <p>The <b>source</b> field of the <b>Event/Alert</b> object should be same as that of the <b>name</b> field of <b>ManagedObject</b> in order to get the ManagedObject's status updated when Alerts are generated.</p> <p><b>Example:</b> Assume you have 10 user PCs in your network. You model each PC as a ManagedObject. Each PC can have failure objects (entities), such as CPU, Monitor, etc.</p> <p>When CPU from User1 fails, you will generate Event with properties, <b>entity = User1_CPU, source = User1</b>.</p> <p>Similarly, when CPU from User2 fails, you will generate Event with properties, <b>entity = User2_CPU, source = User2</b>.</p>
5	<b>domain</b>	\$domain	Represents the domain name for the Event. <i>This field may or may not be used depending on the application.</i>
6	<b>category</b>	\$category	<p>There can be any type of faults reported for an entity. This field can be used to categorize such faults from the same entity.</p> <p><b>Example:</b> Faults reported due to power fluctuation in a device can be in a category called <b>power fluctuation</b> and faults related to CPU usage can be in a category called <b>CPU usage</b>.</p>

7	<b>network</b>	\$network	To set the network name from which the event has to be raised. <i>This may or may not be used depending on the application.</i>
8	<b>node</b>	\$node	The node value for the event. <i>This may or may not be used depending on the application.</i>
9	<b>groupName</b>	\$groupName	Used for grouping purpose.  By default Web NMS framework does not provide any functionality based on groupName of Event object.  But value set for groupName of Event object will be transferred to the Alert object.
10	<b>helpURL</b>	\$helpURL	Holds the URL of the document that contains the details on the event. This is useful in tracking the history of the events generated due to a trap.

## Alarm Properties

S.No.	Property Name	Replaceable Parameter (Property Token)	Description
1	category	\$category	Category value set in the corresponding Event object.
2	createTime	\$createTime	The time when the alarm was created.
3	entity	\$entity	The entity (or failure object) value of the alarm.
4	groupName	\$groupName	Alarms can be grouped based on their similarities. The type of grouping is based on the value set for the parameter GROUP_ALERTS_MODE in NmsProcessesBE.conf.  The values of this parameter can be max, latest, or none. The default setting is none, where the alerts are not grouped.  If the value is set to max, alarms are first grouped and then based on the criticality of the grouped alarms viz., Critical, Major, Minor, etc., alarms of maximum severity are shown at the top of the list.  If the value is set to latest, alarms are grouped. From the grouped alarms, the latest updated alarm's criticality is shown at the top of the list.
5	id	\$id	The ID of the last event that updated the alarm.
6	message	\$message	The message string value of the alarm.
7	modTime	\$modTime	The time the alarm was last modified.  Alarm is the correlation of Events. You have one alarm per entity. Hence, events with the same entity can update the existing alarm. Whenever an alarm is updated with some event, that event's time is updated in the modTime field of alarm.

S.No.	Property Name	Replaceable Parameter (Property Token)	Description
8	previousSeverity	\$previousSeverity	Before each and every alarm update, current severity value is set as the previousSeverity.
9		\$stringpreviousseverity	The previous severity value in string format (e.g., Major and Clear) of the alarm.
10	severity	\$severity	The present severity value (for example., 1, 2, and so on) of the alarm.
11		\$stringseverity	The severity value in string format (for example, Major, Clear, and so on) of the alarm.
12	source	\$source	The source of the alarm.
13	who	\$who	The name of the most recent user who picked up the alarm.

---

## Appendix C: Performance

- 
- Choosing Data Identifiers
  - Adding Statistics at Runtime
- 

### Choosing the Data Identifiers

The following tables explain each of the fields available in the **Poll Details** dialog box. For more information, refer to Defining What Data to Collection.

#### Common Properties

All the Data Identifiers have some common properties which can be specified in this section.

	<b>Note:</b> Currently, Performance Client allows you to specify only two common properties, <b>Prefix</b> and <b>Polling period</b> . You can set the rest in the Configuration file.
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Property	Description
Prefix	<p>Data Identifiers are generally lengthy. For the identifiers that have in common the starting <b>n</b> digits, you can specify that as prefix.</p> <p><b>Example:</b> Assume two Statistics, IfSpeed and IfInOctect. The corresponding Data identifiers are .1.3.6.1.2.1.2.2.1.5.1 and .1.3.6.1.2.1.2.2.1.10.1. Hence you can specify the common prefix as <b>.1.3.6.1.2.1.2.2.1</b>.</p> <p>In the case of <b>RFC 1213 MIB</b>, even if the prefix is not specified, the Performance module will internally add a prefix to the identifier.</p>
Polling Period	<p>The time interval for periodic data collection.</p> <p><b>Example:</b> If set to 5, it indicates that for all the Data Identifiers, data will be collected once in every 5 seconds.</p> <p><b>Default value:</b> 300 seconds</p>

#### Data Identifier Properties

Property	Description
Data Identifier	<p>A unique Object Identifier string that represents a MIB entry. Data is collected for this identifier. An SNMP-specific Data identifier is called <b>OID</b>. This input is mandatory.</p> <p><b>Example:</b> 2.2.1.16.1 refers to IfOutOctects interface of instance 1.</p>
Type	<p>This can be set to <b>interface</b>, <b>node</b>, <b>multiple</b>, or <b>none</b>.</p> <p><b>Note:</b> If you know the fully qualified OID to collect data then you can set the type as <b>Node</b>. <b>Example:</b> If you want to collect data for <b>ifInOctets</b>, <b>instance 1</b> then choose this type and specify the data identifier as <b>.1.3.6.1.2.1.2.2.1.10.1</b></p> <p><b>Interface:</b> This type has been exclusively made available only for IF table entries of RFC 1213 MIB. This is used when the object has many instances. When you want to collect data for all the instances of an object, you can choose the type to</p>

Property	Description
	<p>be <b>Interface</b>. Enter the Data Identifier as <b>.1.3.6.1.2.1.2.2.1.10</b>. For every instance of the object, a PolledData is be created.</p> <p><b>Multiple:</b> If you do not know how many instances exist for the OID then this type can be used to collect data for all the instances. As <b>Interface</b> type is specific to IF table entries, for other OIDs that have multiple instance, you can choose the type as <b>Multiple</b>. Only one PolledData will be created for the specified OID but data collection will be done for all the instances.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Warning:</b> Do not terminate the OID with a dot. If you do so, it will be treated as an invalid OID and data will not be collected for it.       </div> <p><b>None:</b> This is used when other protocols are used for data collection apart from SNMP.</p> <p><b>Default value:</b> None</p>
Name	Any meaningful string for the Data Identifier. It is mandatory.
Protocol	Specify the protocol used - SNMP, TL1, etc. If no value is specified, default protocol <b>SNMP</b> is set.
Interval	<p>The interval for periodic data collection. Example: If set to 2, it indicates that for all the Data Identifiers, data will be collected once in every 2 seconds. <b>Default value:</b> 300 seconds</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note:</b>  <b>Case 1:</b> If polling period (common property) and interval are specified then interval value will take precedence.  <b>Case 2:</b> If polling period is specified but no interval, then polling period will be taken as interval.  <b>Case 3:</b> If neither polling period nor interval is specified, then default value (300 seconds) will be taken.       </div>
Threshold	To apply Threshold on the Data Identifier, select (check) this option. <b>Default value:</b> False
Store Data	Sometimes, you may wish not to store the data collected for the Data Identifier. Hence, you can view the data only by Real Time monitoring using Current Statistic Graph. To specify that you do not want to store the collected data, clear (uncheck) this check box. <b>Default value:</b> True (Checked)
Stats Data Table Name	<p>If the Collected data is of data type <b>Long</b> then it will be stored in STATSDATA table. The table will have the name and current date appended to it. <b>Example:</b> If today's date is Aug 10, 2003 then the table name will be STATSDATA8_10_2003. If you do not specify any input for this property, this will be the default behavior.</p> <p>But if you want to store data in some other table and not in default STATSDATA then you can specify it in this field. <b>Example:</b> MyTable</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Warning:</b> The table name which you specify here must be already available with its structure defined.       </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note:</b> You have to append a percentage symbol (%) to the table name, such as <b>%MyTable%</b>. This enables one table creation per day with the current date appended to the table name. If you do not specify the % symbol, no new table will be created each day and data collected everyday will be appended to the same table <b>MyTable</b>. This results in a voluminous table after some days . It is recommended to have separate tables for each day.       </div>

Property	Description
String Data Table Name	<p>If the Collected data is of data type <b>String</b> then it will be stored in STRINGDATA table. The table will have the name and current date appended to it. <b>Example:</b> If today's date is Aug 10 2003 then the table name will be STRINGDATA8_10_2003. If you do not specify any input for this property , then this will be the default behavior.</p> <p>But if you want to store data in some other table and not in default STRINGDATA then you can specify it in this field. <b>Example:</b> StringMyTable</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Warning:</b> The table name which you specify here must be already available with its structure defined.         </div> <p>The concept of appending % symbol holds good for STRINGDATA table also. For more information, refer to the explanation for the field <b>Stats Data Table Name</b>.</p>
Failure Threshold	<p>This indicates the number of consecutive failures after which, the threshold event should be generated. This can be used when a single Poll (data collection for the Data Identifier) is not stable.</p> <p><b>Example:</b> Assume the Data Identifier has a threshold associated and it is predicted that the data collected can be cross checked 3 times. If the collected value still exceeds the Threshold value then it means that the collected data is stable and this may result in performance degradation.</p> <p><b>Default value:</b> 1</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note:</b> If there are more than one Thresholds associated with the Data Identifier then the collected data has to exceed the same Threshold consecutively <b>n</b> times as specified in this field. Only then the Threshold Event will be generated.         </div>
Save Absolutes	<p>This option is applicable only for <b>Counter type OIDs</b>. By default, data collected for Counter type OIDs is not stored as it is. The difference between the previous data and latest data is collected and stored. If the exact value (absolute value) of collected data has to be stored for Counter type OIDs then this check box should be checked.</p> <p>Data collected for OIDs of other data types are saved as absolute values.</p> <p><b>Default value:</b> False</p>
Time Average	<p>If this option is selected (check), the time average is calculated as <i>(Latest collected value + Previous value) / Difference in Data collection Time value</i>. This is mostly calculated for Counter type and Gauge type Data identifiers where the data collected will be an incremental value and at one point will reach the final value and reset to Zero. As this reset may happen soon and very often, it is preferred that a Delta value is derived from two consecutive polls.</p> <p><b>Default value:</b> false</p>
Active	<p>If this option is not selected (uncheck), data collection will be temporarily stopped for this Data Identifier. To resume data collection you will have to select this field.</p> <p><b>Default value:</b> True (checked)</p>
Save Poll count OID	<p>Specify a number (n) which indicates a count i.e., only after n number of polls, data will be stored in the database. This is used when you feel the initial set of data collected for the Data Identifier is unstable and may not be a correct measure of performance.</p> <p><b>Default value:</b> 1</p>

Property	Description
Save On Threshold	If this option is selected (check), it indicates that the collected data should be saved only when it exceeds threshold. <b>Default value:</b> false (unchecked)
Available Thresholds	This provides a list of Thresholds. Choose one at a time and a comma separated list displayed. <b>Limitation:</b> You cannot associate thresholds specific to an <b>instance</b> of multiple Polled Data created using this user interface. Hence, after creating the Polled Data, set the thresholds to the instances via <b>Modify Statistics UI</b> .



**Note:** SNMP version stored in the Managed Object will be automatically set in the Polled Data.

## Adding Statistics at Runtime

The following table explains each of the fields in the Add Statistics UI. For more information, refer to Adding Statistics at Runtime topic.

Property	Description
Name	Any meaningful string for the Data Identifier. It is a mandatory field.
Snmp Version	<p>One of the three SNMP versions - <b>V1</b>, <b>V2</b> or <b>V3</b>.</p> <ol style="list-style-type: none"> <li>If you choose V3, two more fields labeled User Name and Context Name are available. They are required for authorizing SNMPv3 data collection. For information on configuring security parameters, refer to SNMPV3 Security Configuration topic.</li> <li>If the SNMP agent resides in a proxy implementation environment, it can be accessed via a <b>proxy agent</b>. The SNMP agent, then, has to be identified by a unique value called <b>contextEngineID</b>. This value has to be set as a user property for the Statistic.</li> </ol> <p><b>Default value:</b> v1</p>
Community	Specify the string using which the devices are identified in a network. Most of the equipment vendors set the Community value as <b>public</b> for their devices. In such case, specify this field as <b>public</b> . Otherwise, you need to check the string used for the particular device.
Agent	<p>Normally, a device will have one agent in it to collect device data, where device name and agent name will be same. Hence, you can specify the device name as agent name. <b>Example:</b> switch-rk4.</p> <p><b>Note:</b></p> <ol style="list-style-type: none"> <li>If you are adding Statistic via UI, ensure that agent name and DNS name are set.</li> <li>For collecting data from a TL1 node residing behind a TL1 gateway, specify the TargetID of the TL1 node. This is to facilitate Poll Engine for grouping the data requests based on APP (Agent+Period+Protocol) combination.</li> </ol>
Port	Specify the port number to which Web NMS can send the request for data collection. Default SNMP agent port is <b>161</b> . If no value is specified, the default port 161 is set when PolledData is created.

Property	Description
	If multiple agents are running in the same device, they have to be differentiated by different port numbers.
OID	A unique Object Identifier string that represents a MIB entry. Data is collected for this identifier. An SNMP-specific Data identifier is called <b>OID</b> . For example, 2.2.1.16.1 refers to IfInOctets interface instance 1. You can also specify an expression OID. This input is mandatory.  For collecting data from a TL1 node residing behind a TL1 gateway, specify the TL1 command which in turn should consist the TargetID of the TL1 node. TL1 Gateway parses this command, extracts the TargetId, and identifies the TL1 node from which to collect data.
Active	If you do not select (uncheck) this option, data collection will not start for this OID.  <b>Default value:</b> True (checked)
Period	The time interval for periodic data collection. <b>Example:</b> If set to 2, it indicates that for all the Data Identifiers, data will be collected once in every 2 seconds.  <b>Default value:</b> 300 seconds  You can configure the minimum period so that the period cannot be set for a Statistic less than the minimum period. This can be done by setting the property <b>MIN-PERIOD</b> in <b>Tree.xml</b> (located in the <Web NMS Home>/users/root directory ) for the entry <b>MODULE-NAME = "Stats Admin"</b> .  <b>Example:</b> <b>MIN-PERIOD = "200"</b> . Henceforth, if you enter the period less than the minimum period set, an error message will be displayed.
Threshold	To apply threshold on this Statistics, select (check) this field  <b>Default value:</b> False (unchecked)  The list of Thresholds can be specified in the text box labeled Threshold List.
DNS Name	Specify the name of the device from which data has to be collected. <b>Example:</b> switch-rk4  DNS name field is mandatory for TL1 nodes that are behind a TL1 Terminal Server.
Save	If this option is not selected, data will be collected but will not be stored in the database.  <b>Default value:</b> True (Checked)
Save Absolutes	This option is applicable only for <b>Counter type OIDs</b> . By default, data collected for Counter type OIDs is not stored as it is. The difference between the previous data and latest data is collected and stored. If the exact value (absolute value) of collected data has to be stored for Counter type OIDs then this option should be selected (checked).  Data collected for OIDs of other data types is saved as absolute values.  <b>Default value:</b> False
Log Directly	To store the collected data in flat files rather than storing them in database, select this option.  <b>Default value:</b> false (unchecked) You can set the log filename in the text box labeled Log file.

Property	Description
User Name	Specify a string value which is matched with agent's list of users who are authorized to collect data from it. This field is displayed only when Snmp Version is selected as V3.
Context Name	Specify the string value that authenticates the user. This text box will be displayed only when Snmp Version is selected as V3.

Property	Description
Log file	Specify the log filename with full path, i.e., location on hard disk where the log file has to be stored.
Parent Obj	Specify the name of the Managed Object which acts as the parent for this Statistic.
Threshold List	<p>Specify the name of the Thresholds as comma-separated values thus associating them with this Statistic for monitoring data collection.</p> <p>In case of multiple Polled Data, if you need to associate Thresholds specific to the instances then specify the association as follows:</p> <pre>&lt;instance number&gt;=thresholdname1,thresholdname2, ....: &lt;instance number&gt;=thresholdname1,thresholdname2, ....</pre> <p><b>Example:</b></p> <pre>.1=th1,th2:.2=th1,th3</pre> <p>The specified list of Thresholds will be applied on the Statistic only when Threshold property is <b>true</b>.</p>
Current save count	This is used for internal purpose.
Protocol	Specify the protocol used for data collection - SNMP, TL1, etc. When no value is set, default protocol <b>SNMP</b> is assumed for data collection.
Statsdata Table Name	<p>If the Collected data is of data type <b>Long</b>, it will be stored in STATSDATA table. The table will have the name and current date appended to it. <b>Example:</b> If today's date is Aug 10, 2003 then the table name will be STATSDATA8_10_2003. If you do not specify any input for this property, this will be the default behavior.</p> <p>If you want to store data in some other table other than the default STATSDATA, specify it in this field. <b>Example:</b> MyTable.</p> <p>Append a percentage symbol (%) to the table name, such as MyTable%. This enables one table creation per day with the current date appended to the table name. If you do not specify the % symbol, new table is not created and data collected everyday will be appended to the same table MyTable. This results in a voluminous table after some days. It is recommended to have separate tables for each day.</p> <p><b>Warning:</b> The table name which you specify here must be already available in the database.</p>
Save PollCount	<p>Specify an integer (n). During every <b>nth</b> Poll, the collected data will be stored. <b>Example:</b> If you specify 2, it indicates that for every alternate polling the collected data is stored, i.e., 2nd poll, 4th poll, and so on.</p> <p><b>Default value:</b> 1</p>

Property	Description
Failure Threshold	<p>This indicates the number of consecutive failures after which the threshold event should be generated.</p> <p><b>Example:</b> Assume the OID has a threshold associated and it is predicted that the data collected can be cross-checked 3 times. If the collected value still exceeds the Threshold value then corresponding Threshold event will be generated.</p> <p><b>Default value:</b> 0</p> <p>If there are more than one Threshold associated with the Data identifier, then the collected data has to exceed the same threshold consecutively n times as specified in this field. Only then the Threshold Event will be generated.</p>
Is multiple PolledData	Select this option if Data Identifier is of type <b>multiple</b> .
Save On Threshold	Possible values are <b>true</b> and <b>false</b> . If set <b>true</b> , the collected data is saved only when it exceeds threshold.
Owner name	Specify a string to denote the owner of the Statistic.
Time Avg	<p>If this option is selected (checked) the Time Average is calculated as</p> $\frac{(\text{Latest collected value} - \text{Previous value})}{\text{Difference in Data collection Time value}}$ <p>This is mostly calculated for Counter type OIDs where the collected data will be an incremental value and at one point will reach the final value and reset to Zero. As this reset may happen soon and very often, it is preferred that a Delta value is derived from two consecutive Polls.</p> <p><b>Default value:</b> false</p>