APPENDIX A

CLI Tools

This section explains all the CLI utilities that are available for the administrator in LMS 4.2.

This section contains:

- Setting Up Local Users Through CLI
- Changing Cisco Prime User Password Through CLI
- Managing Processes Through CLI
- Working With Third Party Security Certificates
- Setting up Browser-Server Security
- Backing up Data Using CLI
- Using LMS Server Hostname Change Scripts
- Using DCR Features Through CLI
- Using Group Administration Features Through CLI
- Deleting Stale Groups Using CLI
- User Tracking Command Line Interface
- Using Lookup Analyzer Utility
- Understanding UTLite
- User Tracking Debugger Utility
- Configuring Switches to Send MAC Notifications to LMS Server
- Administration Command Line Interface

Setting Up Local Users Through CLI

You can set up the local users through CLI. This feature helps you in:

- Adding Local Users
- Importing Local Users
- Importing Users From ACS
- Migrating User Details from LMS 3.2 to LMS 4.x versions

Adding Local Users

You can add bulk local users through CLI. This feature allows you to specify a file that has information about the local users as an input. The input file you use should be a plain text file.

Note You can use this CLI command for both system and user-defined roles.

Each local user information should be represented in the following format in the text file:

Username:Password:E-mail:Roles:DeviceUname:DevicePassword:DeviceEnPassword

where,

- *Username* — Local username. The local username is case-insensitive.
- *Password* — Password for the local user account name.

  You can leave this field blank in the text file and enter the password in the command line when you run the CLI utility.

  Note that you should enter the password either in the command line or in the input text file. If you mention the password in both the places, the local user will be added with the password specified in the command line. On adding the user by giving password in the command line prompt, default role will be assigned to the user if the role is missing in the input file.
- *E-mail* — E-mail address of the local user.

  This is mandatory if you assign the approver role to the local user. Otherwise, this is optional.
- *Roles* — Roles to be assigned to the local user. You should assign one or more of the following roles to the user separated by comma.
  - Help Desk
  - Approver
  - System Administrator
  - Network Administrator
  - Network Operator
  - Super Admin
- *DeviceUname*—Device login username
- *DevicePassword*—Device login password
- *DeviceEnPassword* —Device enable password.

The following is an example of local user information to be represented in input text file:

```
admin123:admin123:admin123@cisco.com:Help Desk,System
Administrator:admin:roZes123:roZes
```

To add local users through CLI, enter the following commands:

- *NMSROOT*`/bin/perl` *NMSROOT*`/bin/AddUserCli.pl -add` *Filename Password* (on Solaris/Soft Appliance)
- *NMSROOT*`\bin\perl` *NMSROOT*`\bin\AddUserCli.pl -add` *Filename Password* (on Windows)

where,

- *Filename* — Absolute path of the filename containing local users information.
- *Password* — Common password for all user accounts specified in the input text file.

  This command line parameter is optional if you have specified the passwords for local users in the input text file. Note that you should enter the password either in the command line or in the input text file.

  If you specify this parameter, the local users are added to Cisco Prime only with this password irrespective of the password entries specified in the input text file.

For example, enter the following command to add local users mentioned in the input file **localuser.txt** with the password **admin**:

```
C:\progra~1\CSCOpx\bin\perl C:\progra~1\CSCOpx\bin\AddUserCli.pl -add
C:\files\localuser.txt admin
```

Even if you have entered password for the local users in the **localuser.txt** file, the local users are added with the password mentioned in the command line.

Importing Local Users

This feature allows you to import local user information to the local server from a remote LMS Server.

You can import local users from ACS through CLI. See, Importing Users From ACS for more information.

You should have the privileges to import local users from remote LMS Server through CLI.

Before you import users from a remote server, you should install the peer certificate of the remote server in the local LMS Server, if the LMS Server is in HTTPS mode. See Setting up Peer Server Certificate for more information.

To import users from a remote server, enter the following commands:

- *NMSROOT*`/bin/perl` *NMSROOT*`/bin/AddUserCli.pl -import` *Protocol Hostname Portnumber Username Password* (on Solaris/Soft Appliance)
- *NMSROOT*`\bin\perl` *NMSROOT*`\bin\AddUserCli.pl -import` *Protocol Hostname Portnumber Username Password (*on Windows)

where,

- *Protocol* — Protocol of the remote LMS Server.

  The supported values are HTTP or HTTPS.
- *Hostname* — Hostname or IP Address of the remote LMS Server.
- *Portnumber* — Port Number of the remote LMS Server.
- *Username* — Remote LMS Server Login Username.
- *Password* — Remote LMS Server Login Password.

For example, enter the following command to import the local users from the remote LMS Server **lmsdocpc**:

```
NMSROOT\bin\perl NMSROOT\bin\AddUserCli.pl -import HTTP lmsdocpc 1741 admin admin
```

Importing Users From ACS

To import users from ACS through CLI, enter the following commands:

- *NMSROOT*`/bin/perl` *NMSROOT*`/bin/AddUserCli.pl -importFromAcs` *Filename Password* (on Solaris/Soft Appliance)
- *NMSROOT*`\bin\perl` *NMSROOT*`\bin\AddUserCli.pl -importFromAcs` *Filename Password* (on Windows)

where,

- *Filename* — Ouput of executing CSUtil.exe.
- *Password* — ACS password which is the default password assigned to all users.

Migrating User Details from LMS 3.2 to LMS 4.x versions

To migrate user details from LMS 3.2 to LMS 4.x:

Step 1 Enter the command given below:

For Solaris and Soft Appliance:

```
/NMSROOT/lib/jre/bin/java -cp
/NMSROOT/lib/classpath:/NMSROOT/www/classpath:/NMSROOT/MDC/tomcat/shared/lib/
castor-0.9.5-xml.jar:/NMSROOT/MDC/tomcat/shared/lib/castor-0.9.5.jar
com.cisco.nm.cmf.servlet.CWPassMigration <cwpass file location> <output file name with .xml
extension>
```

where, NMSROOT is the directory where you have installed Cisco Prime.

Example:

```
/opt/CSCOpx/lib/jre/bin/java -cp
/opt/CSCOpx/lib/classpath:/opt/CSCOpx/www/classpath:/opt/CSCOpx/MDC/tomcat/shared/lib/
castor-0.9.5-xml.jar:/opt/CSCOpx/MDC/tomcat/shared/lib/castor-0.9.5.jar
com.cisco.nm.cmf.servlet.CWPassMigration /cwpass /output.xml
```

For Windows:

```
/NMSROOT/lib/jre/bin/java -cp
/NMSROOT/lib/classpath;/NMSROOT/www/classpath;/NMSROOT/MDC/tomcat/shared/lib/
castor-0.9.5-xml.jar;/NMSROOT/MDC/tomcat/shared/lib/castor-0.9.5.jar
com.cisco.nm.cmf.servlet.CWPassMigration <cwpass file location> <output file name with .xml
extension>
```

where, NMSROOT is the directory where you have installed Cisco Prime.

Example:

```
C:/Progra~1/CSCOpx/lib/jre/bin/java -cp
C:/Progra~1/CSCOpx/lib/classpath;C:/Progra~1/CSCOpx/www/classpath;C:/Progra~1/CSCOpx/MD
C/tomcat/shared/lib/castor-0.9.5-xml.jar;C:/Progra~1/CSCOpx/MDC/tomcat/shared/lib/
castor-0.9.5.jar com.cisco.nm.cmf.servlet.CWPassMigration C:/cwpass C:/output.xml
```

Step 2 Move the output file to the client machine to import the user details.

Step 3 Go to **Admin > System > User Management > Local User Setup.**

The Local User Setup page appears.

Step 4 Click **Import Users.**

Step 5 Click **Browse** and select the output file from the client machine.

Step 6 Click **Submit**.

Migrating User Details using Selective Backup Method

The user details can be migrated from LMS 3.2 to LMS 4.x versions by remote upgrade procedure. The inline upgrade does not support the direct migraiton of user details from LMS 3.2 to LMS 4.2.

Step 1 Take selective backup from LMS 3.2 using the command given below:

NMSROOT`\bin>perl` *NMSROOT*`\bin\backup.pl -dest=` <*Backup Directory*> `-system`

where, NMSROOT is the directory where you have installed Cisco Prime.

Step 2 Move the backup to LMS 4.x server where data has to be restored.

Step 3 Stop the daemons on 4.x server

Step 4 Restore backup using the command given below:

NMSROOT`\bin>perl` *NMSROOT*`\bin\restorebackup.pl -d` <*Backup Directory*>

Step 5 Check for any errors on **Restorebackup.log**

Step 6 Start the daemons and check the user details once all the processes are up.

Note Selective backup includes system settings, user details and jobs.

Changing Cisco Prime User Password Through CLI

You can change the Cisco Prime user password using the Cisco Prime user password recovery utility.

To change the user password on Solaris/Soft Appliance:

Step 1 Enter `/etc/init.d/dmgtd stop` to stop the Daemon Manager.

Step 2 Set the LD_LIBRARY_PATH manually. The path is to be set as follows:

```
setenv LD_LIBRARY_PATH /opt/CSCOpx/MDC/lib:/opt/CSCOpx/lib
```

This environment variable set is applicable to the current working shell only.

Now, you can change the password using the Cisco Prime user password recovery utility.

Step 3 Enter *NMSROOT*`/bin/resetpasswd` *username* at the command prompt.

Here *NMSROOT* refers to the Cisco Prime Installation directory.

A message appears:

```
Enter new password for username:
```

Step 4 Enter the new password.

Step 5 Enter **`/etc/init.d/dmgtd start`** to start the Daemon Manager.

To change the user password on Windows:

Step 1 Enter **`net stop crmdmgtd`** to stop the Daemon Manager.

Step 2 Enter *NMSROOT*`\bin\resetpasswd` *username* at the command prompt.

A message appears:

```
Enter new password for username:
```

Step 3 Enter the new password.

Step 4 Enter **`net start crmdmgtd`** to start the Daemon Manager.

Managing Processes Through CLI

You can also manage the Cisco Prime processes through CLI. You can perform the following activities through CLI:

- Viewing Process Details Through CLI
- Viewing Brief Details of Processes
- Viewing Processes Statistics
- Starting a Process
- Stopping a Process

Viewing Process Details Through CLI

The **`pdshow`** command displays the details of the specified processes or all processes in the CLI prompt.

- To display the details of all processes, enter:
  - **`/opt/CSCOpx/bin/pdshow`** (on Solaris/Soft Appliance)
  - **`pdshow`** (on Windows)
- To display the details of one or more specified processes, enter:
  - **`/opt/CSCOpx/bin/pdshow`** *ProcessName1 ProcessName2* (on Solaris/Soft Appliance)
  - **`pdshow`** *ProcessName1 ProcessName2* (on Windows)

    where *ProcessName1* and *ProcessName2* are the name of the processes.

The command displays the process details of one or more processes. See Viewing Process Details for description of each of these items.

- Process Name
- Process State
- Process ID
- Process Return Code
- Process Signal Number
- Process Start Time
- Process Stop Time

The **pdshow** command additionally displays the following process details.

Process Details	Description
Core	*Not applicable* means the program is running normally. *CORE FILE CREATED* means the program is not running normally and the operating system has created a file called *core**. The core file stores important data about processes. *core** refers to the name of the core file. The core file name contains the executable file name of the program and the process ID. For example, the name of the core file created for the Perl module is: `core.perl.51234`
Information	Describes what the process is doing and how it is started. *Not applicable* means the program is not running normally.

During the startup of Daemon Manager, sometimes the **pdshow** command may display information message requesting you to wait and enter the command again.

This happens particularly when the Daemon Manager is busy in running the tasks one by one in the queue. You must enter the command again to view the process details.

Viewing Brief Details of Processes

The **pdshow -brief** command displays the brief status of all processes or specified processes in tabular format in the CLI prompt.

- To display the brief details of all processes, enter:
  - **/opt/CSCOpx/bin/pdshow -brief** (on Solaris/Soft Appliance)
  - **pdshow -brief** (on Windows)
- To display the details of one or more specified processes, enter:
  - **/opt/CSCOpx/bin/pdshow -brief** *ProcessName1 ProcessName2* (on Solaris/Soft Appliance)
  - **pdshow -brief** *ProcessName1 ProcessName2* (on Windows)

    where *ProcessName1* and *ProcessName2* are the name of the processes.

The command displays the following details in tabular format:

- Process Name
- Process State
- Process ID

For example, if you enter **/opt/CSCOpx/bin/pdshow -brief Tomcat Apache** in the command prompt, the following output is displayed:

```
ProcessStatePid
***************
Tomcat     Program Started - No mgt msgs received13824
Apache     Running normally                      13847
```

Viewing Processes Statistics

The `pdshow -stat` command displays the statistics of all processes or specified processes in tabular format.

Note You can enter this command only on Solaris systems.

To display the brief details of all processes, enter:

`/opt/CSCOpx/bin/pdshow -stat` (on Solaris/Soft Appliance)

To display the details of one or more specified processes, enter:

`/opt/CSCOpx/bin/pdshow -stat` *ProcessName1 ProcessName2* (on Solaris/Soft Appliance)

where *ProcessName1* and *ProcessName2* are the name of the processes.

The command displays the following details in tabular format in the command line.

Process Details	Description
Pid	Process ID
%CPU	CPU usage of a process at a particular time expressed in terms of percentage
RSS	Resident set size displayed in terms of KB
VSZ	Virtual memory size of process displayed in terms of KB
%MEM	Ratio of resident set size and physical memory expressed in terms of percentage
NLWP	Number of light weight processes of the specified process
Process	Name of the process

Starting a Process

You must enter the following commands to start a process through CLI:

- `/opt/CSCOpx/bin/pdexec` *ProcessName* (on Solaris/Soft Appliance)
- `pdexec` *ProcessName* (on Windows)

The dependent processes are started first before the specified process is started.

If the process is being restarted after a shutdown, any dependent processes registered with the Daemon Manager is not automatically restarted. Dependent processes are automatically restarted only when the Daemon Manager itself is restarted.

Stopping a Process

You must enter the following commands to stop a process through CLI:

- `/opt/CSCOpx/bin/pdterm` *ProcessName (on Solaris/Soft Appliance)*
- `pdterm` *ProcessName* (on Windows)

The dependent processes are also shut down using this CLI command.

Working With Third Party Security Certificates

Cisco Prime provides an option to use security certificates issued by third party certificate authorities (CAs). You may want to use this option in cases where your organizational policy prevents you from using Cisco Prime self-signed certificates or requires you to use security certificates obtained from a particular CA.

You can use these certificates to enable SSL when you need secure access between LMS Server and your client browser. You can do the following:

- Uploading Third Party Security Certificates to LMS Server
- Using the SSL Utility Script to Upload Third Party Security Certificates

Uploading Third Party Security Certificates to LMS Server

You can upload Third Party Security Certificates using the SSL Utility Script.

Note Cisco Prime does not support third-party certificates with "Subject Alternative Names".

This utility is available at:

- *NMSROOT*\MDC\Apache (On Windows)
- *NMSROOT*/MDC/Apache/bin (On Solaris/Soft Appliance)

Note The maximum supported public key value is 1024 bits.

This utility has the following options:

Number	Option	What it Does...
1	Display LMS Server certificate information	• Displays the Certificate details of the LMS Server. For third party issued certificates, this option displays the details of the server certificate, the intermediate certificates, if any, and the Root CA certificate. • Verifies if the certificate is valid.
2	Display the input certificate information	This option accepts a certificate as an input and: • Verifies whether the certificate is in encoded X.509 certificate format. • Displays the subject of the certificate and the details of the issuing certificate. • Verifies whether the certificate is valid on the server.
3	Display Root CA certificates trusted by LMS Server	Generates a list of all Root CA Certificates.

Number	Option	What it Does... (continued)
4	Verify the input certificate or certificate chain	Verifies whether the server certificate issued by third party CAs, can be uploaded. When you choose this option, the utility: • Verifies if the certificate is in Base64 Encoded X.509Certificate format. • Verifies if the certificate is valid on the server • Verifies if the server private key and input server certificate match. • Verifies if the server certificate can be traced to the required Root CA certificate using which it was signed. • Constructs the certificate chain, if the intermediate chains are also given, and verifies if the chain ends with the proper Root CA certificate. After the verification is successfully completed, you are prompted to upload the certificates to LMS Server. The utility displays an error: • If the input certificates are not in required format • If the certificate date is not valid or if the certificate has already expired. • If the server certificate could not be verified or traced to a root CA certificate. • If any of the intermediate Certificates were not given as input. • If the server private key is missing or if the server certificate that is being uploaded could not be verified with the server private key. You must contact the CA who issued the certificates to correct these problems before you upload the certificates to Cisco Prime.

Number	Option	What it Does... (continued)
5	Upload single server certificate to LMS Server	You must verify the certificates using option 4 before you select this option. Select this option, only if there are no intermediate certificates and there is only the server certificate signed by a prominent Root CA certificate. If the Root CA is not one trusted by Cisco Prime, do not select this option. In such cases, you must obtain a Root CA certificate used for signing the certificate from the CA and upload both the certificates using option 6. When you select this option, and provide the location of the certificate, the utility: • Verifies whether the certificate is in Base64 Encoded X.509 certificate format. • Displays the subject of the certificate and the details of the issuing certificate. • Verifies whether the certificate is valid on the server. • Verifies whether the server private key and input server certificate match. • Verifies whether the server certificate can be traced to the required Root CA certificate that was used for signing. After the verification is successfully completed, the utility uploads the certificate to LMS Server. The utility displays an error: • If the input certificates are not in required format • If the certificate date is not valid or if the certificate has already expired. • If the server certificate could not be verified or traced to a root CA certificate. • If the server private key is missing or if the server certificate that is being uploaded could not be verified with the server private key. You must contact the CA who issued the certificates to correct these problems before you upload the certificates in Cisco Prime again.

Number	Option	What it Does... (continued)
6	Upload a certificate chain to LMS Server	You must verify the certificates using option 4 before you select this option. Select this option, if you are uploading a certificate chain. If you are also uploading the root CA certificate also, you must include it as one of the certificates in the chain. When you select this option and provide the location of the certificates, the utility: • Verifies whether the certificate is in Base64 Encoded X.509 Certificate format. • Displays the subject of the certificate and the details of the issuing certificate. • Verifies whether the certificate is valid on the server • Verifies whether server private key and the server certificate match. • Verifies whether the server certificate can be traced to the root CA certificate that was used for signing. • Constructs the certificate chain, if intermediate chains are given and verifies if the chain ends with the proper root CA certificate. After the verification is successfully completed, the server certificate is uploaded to LMS Server. All the intermediate certificates and the Root CA certificate are uploaded and copied to the Cisco Prime TrustStore. The utility displays an error: • If the input certificates are not in required format. • If the certificate date is not valid or if the certificate has already expired. • If the server certificate could not be verified or traced to a root CA certificate. • If any of the intermediate certificates were not given as input. • If the server private key is missing or if the server certificate that is being uploaded could not be verified with the server private key. You must contact the CA who issued the certificates to correct these problems before you upload the certificates in Cisco Prime again.
7	Modify Certificate	This option allows you to modify the Host Name entry in the LMS Certificate. You can enter an alternate Hostname if you wish to change the existing Host Name entry.

Using the SSL Utility Script to Upload Third Party Security Certificates

To upload the certificates:

Step 1 Stop the Daemon Manager from the Cisco Prime CLI:

On Windows:

- Enter **`net stop crmdmgtd`**

On Solaris/Soft Appliance:

- Enter **`/etc/init.d/dmgtd stop`**

Step 2 Navigate to the directory where the SSL Utility script is located.

On Windows:

a. Go to *NMSROOT*\MDC\Apache

b. Enter *NMSROOT*\**`bin\perl SSLUtil.pl`**

On Solaris/Soft Appliance:

a. Go to *NMSROOT*/MDC/Apache/bin

b. Enter *NMSROOT*/**`bin/perl SSLUtil.pl`**

Step 3 Select option **4**, Verify the input Certificate or Certificate Chain.

Step 4 Enter the location of the certificates (server certificate and intermediate certificate).

The script verifies if the server certificate is valid. After the verification is complete, the utility displays the options.

If the script reports errors during validation and verification, the SSL Utility displays instructions to correct these errors. Follow the instructions to correct those errors and then try to upload the certificates.

Step 5 Select option **5**, if you have only one certificate to upload, that is if you have a server certificate signed by a Root CA certificate.

Or

Select option **6**, if you have a certificate chain to upload, that is if you have a server certificate and intermediate certificates.

Cisco Prime does not allow you to proceed with the upload if you have not stopped the Cisco Prime Daemon Manager.

The utility displays a warning message if there are hostname mismatches detected in the server certificate being uploaded, but you can continue to upload the certificate.

Step 6 Enter the following required details:

- Location of the certificate
- Location of intermediate certificates, if any.

SSL Utility uploads the certificates, if all the details are correct and the certificates meet Cisco Prime requirements for security certificates.

Step 7 Restart the Daemon Manager for the new security certificate to take effect.

Enable SSL to establish a secured connection between LMS Server and your client browser, if you have not enabled already.

Note The maximum supported public key value is 1024 bits.

Note Cisco Prime does not support third-party certificates with “Subject Alternative Names”.

Setting up Browser-Server Security

This section contains:

- Enabling Browser-Server Security From the Command Line Interface (CLI) On Windows Platforms
- Enabling Browser-Server Security From the Command Line Interface (CLI) On Solaris/Soft Appliance Platforms
- Disabling Browser-Server Security From the Command Line Interface (CLI) On Windows Platforms
- Disabling Browser-Server Security From the Command Line Interface (CLI) On Solaris/Soft Appliance Platforms

Enabling Browser-Server Security From the Command Line Interface (CLI) On Windows Platforms

To enable Browser-Server Security from CLI:

Step 1 Go to the command prompt.

Step 2 Navigate to the directory *NMSROOT*\MDC\Apache.

Step 3 Enter *NMSROOT*`\bin\perl ConfigSSL.pl -enable`

Step 4 Press **Enter**.

- If you have the required security certificates available on the server, Cisco Prime enables SSL.
- If you do not have the security certificates on the server, Cisco Prime prompts you to create your own self-signed certificate and enter the details required to create a self-signed certificate.

Step 5 Create a self-signed certificate or use certificates you obtained from a Certification Authority (CA).

The LMS Server creates the security certificate. You can use this certificate to enable SSL in the LMS Server from your client browser.

Step 6 Log out from your Cisco Prime session, and close all browser sessions.

Step 7 Restart the Daemon Manager from the LMS Server CLI:

a. Enter `net stop crmdmgtd`

b. Enter `net start crmdmgtd`

Step 8 Restart the browser, and the Cisco Prime session.

When you restart the Cisco Prime session after enabling SSL, you must enter the URL with the following changes:

- The URL should begin with **https** instead of **http** to indicate secure connection. Cisco Prime will automatically redirect you to HTTPS mode if SSL is enabled.
- Change the port number suffix from **1741** to **443**.

If you do not make the above changes, LMS Server will automatically redirect you to **HTTPS** mode with port number 443. The port numbers mentioned above are applicable for LMS Server running on Windows.

Enabling Browser-Server Security From the Command Line Interface (CLI) On Solaris/Soft Appliance Platforms

To enable Browser-Server Security from CLI:

Step 1 Go to the command prompt.

Step 2 Navigate to the directory *NMSROOT*\MDC\Apache\bin.

Step 3 Enter `./ConfigSSL.pl -enable`

Step 4 Press **Enter**.

- If you have the required security certificates available on the server, Cisco Prime enables SSL.
- If you do not have the security certificates on the server, Cisco Prime prompts you to create your own self-signed certificate and enter the details required to create a self-signed certificate.

Step 5 Create a self-signed certificate or use certificates you obtained from a Certification Authority (CA).

The LMS Server creates the security certificate. You can use this certificate to enable SSL in the LMS Server from your client browser.

Step 6 Log out from your Cisco Prime session, and close all browser sessions.

Step 7 Restart the Daemon Manager from the LMS Server CLI:

a. Enter `/etc/init.d/dmgtd stop`

b. Enter `/etc/init.d/dmgtd start`

Step 8 Restart the browser, and the Cisco Prime session.

When you restart the Cisco Prime session after enabling SSL, you must enter the URL with the following changes:

- The URL should begin with **https** instead of **http** to indicate secure connection. Cisco Prime will automatically redirect you to HTTPS mode if SSL is enabled.
- Change the port number suffix from **1741** to **443**.

If your LMS Server is integrated with any Network Management Station (NMS) in your network using the integration utility (NMIM), you must perform the integration every time you enable or disable SSL in the LMS Server. This is required to update the application registration in NMS.

For more information, see the Integration Utility Online Help.

Disabling Browser-Server Security From the Command Line Interface (CLI) On Windows Platforms

To disable Browser-Server Security from CLI:

Step 1 Go to the command prompt.

Step 2 Navigate to the directory *NMSROOT*\MDC\\Apache.

Step 3 Enter *NMSROOT*`\bin\perl ConfigSSL.pl -disable`

Step 4 Press **Enter**.

Step 5 Log out from your Cisco Prime session, and close all browser sessions.

Step 6 Restart the Daemon Manager from the LMS Server CLI:

a. Enter `net stop crmdmgtd`

b. Enter `net start crmdmgtd`

Step 7 Restart the browser, and the Cisco Prime session.

When you restart the Cisco Prime session after disabling SSL, you must enter the URL with the following changes:

- The URL should begin with **http** instead of **https** to indicate that connection is not secure.
- Change the port number suffix from **443** to **1741**.

The port numbers mentioned above are applicable for LMS Server running on Windows.

Disabling Browser-Server Security From the Command Line Interface (CLI) On Solaris/Soft Appliance Platforms

To disable Browser-Server Security from CLI:

Step 1 Go to the command prompt.

Step 2 Navigate to the directory *NMSROOT*\MDC\\Apache\\bin.

Step 3 Enter ./`ConfigSSL.pl -disable`

Step 4 Press **Enter**.

Step 5 Log out from your Cisco Prime session, and close all browser sessions.

Step 6 Restart the Daemon Manager from the LMS Server CLI:

a. Enter `/etc/init.d/dmgtd stop`

b. Enter `/etc/init.d/dmgtd start`

Step 7 Restart the browser, and the Cisco Prime session.

When you restart the Cisco Prime session after disabling SSL, you must enter the URL with the following changes:

- The URL should begin with **http** instead of **https** to indicate that connection is not secure.
- Change the port number suffix from **443** to **1741**.

If your LMS Server is integrated with any Network Management Station (NMS) in your network using the Integration Utility (NMIM), you must perform the integration every time you enable or disable SSL in the LMS Server. This is required to update the application registration in NMS.

For more information, see *Integration Utility Online Help*.

Backing up Data Using CLI

To back up data using CLI on Windows and Solaris/Soft Appliance:

On Windows, run:

```
NMSROOT\bin\perl NMSROOT\bin\backup.pl BackupDirectory [LogFile]
email=[comma_separated_email_ids] [Num_Generations]
```

On Solaris/Soft Appliance, run:

```
/opt/CSCOpx/bin/perl /opt/CSCOpx/bin/backup.pl BackupDirectory [LogFile]
email=[comma_separated_email_ids] [Num_Generations]
```

where,

- *BackupDirectory*—Directory that you want to be your backup directory. This is mandatory.
- *LogFile*— Log file name that contains the details of the backup
- *comma_separated_email_ids*—Email IDs seperated by comma
- *Num_Generations*—Maximum backup generations to be kept in the backup directory.

To back up only selective data using CLI on Windows and Solaris/Soft Appliance:

On Windows, run:

```
NMSROOT\bin\perl NMSROOT\bin\backup.pl -dest=BackupDirectory -system
[-log=LogFile] -gen=Num_Generations]
```

On Solaris/Soft Appliance, run:

```
/opt/CSCOpx/bin/perl /opt/CSCOpx/bin/backup.pl -dest=BackupDirectory -system
[-log=LogFile] [-gen=Num_Generations]
```

where,

- `-dest=`*BackupDirectory*—Directory where the backed up data to be stored. This is mandatory.
- `-system`—Command line option that allows you to back up only the selected system configurations from all applications instead of backing up the complete databases. This is mandatory.
- `-log=`*LogFile*— Log file name that contains the details of the backup.
- `-gen=`*Num_Generations*—Maximum backup generations to be retained in the backup directory.

Using LMS Server Hostname Change Scripts

When you change the hostname of the LMS Server, you need to change the hostname related entries in the Cisco Prime directories and files, registry entries, and databases.

LMS provides a CLI utility to update the new hostname information in the LMS related directories and files, registry entries, and databases, after you have changed your hostname.

You can use the `hostnamechange.pl` script to update the hostname changes in all files, database entries and registry entries.

Caution Make sure that you run this command after you have changed your hostname and the appropriate entries specific to the operating system are updated.

Prerequisites

Before running the hostname change script, you should do the following:

Step 1 Update the hostname entries specific to operating system in your machine.

On Solaris:

- /etc/hosts - Modify loghost to the new hostname.
- /etc/hostname.hm0 or the appropriate interface file - Modify the file to the new hostname.
- /etc/nodename or the appropriate interface file - Modify nodename to the new hostname.

  For Solaris/Soft Appliance, the **`sys-unconfig`** command erases the hostname and IP addresses pertaining to the Solaris/Soft Appliance system (not the LMS or SMS software) and guides you through the server-renaming process. You can also do this when you change the hostname in the hosts, hostname.hme0, and nodename files in the /etc directory.

On Soft Appliance:

To change the hostname in Soft Appliance operating system:

a. Login to vSphere client.

b. Select the server where you want to Run hostnamechange.pl.

c. Login to the selected server as system admin.

d. Stop the daemons before changing the hostname in CARS CLI, by runing the command `/etc/init.d/dmgtd stop` in shell mode.

e. Enter “config terminal” in the console.

Config prompt appears. Enter “hostname <*new host name*>”

f. Exit from the configure prompt.

g. Enter “write memory”.

On Windows:

To change the hostname in Windows operating system:

a. Right-click the My Computer icon from the desktop and click **System Properties**.

Or

Click **Start > Settings > Control Panel > System**.

The System Properties dialog box opens.

b. Click the Computer Name tab.

c. Click **Change...** on the Windows 2008 machine to open the Computer Name Changes dialog box.

d. Enter the new hostname in the Computer Name field.

e. Click **OK** to go back to System Properties dialog box.

f. Click **Apply** to apply the changes.

Step 2 Restart the machine.

You must restart the machine when you:

- Update the operating system specific hostname entries.

Step 3 Stop the Daemon Manager by entering the following commands:

- **`/etc/init.d/dmgtd stop`** (on Solaris/Soft Appliance)

- **`net stop crmdmgtd`** (on Windows)

Step 4 Run the hostname script without command line options. See Running the Hostname Change Script for more information.

Step 5 Start the Daemon Manager by entering the following commands:

- **`/etc/init.d/dmgtd start`** (on Solaris/Soft Appliance)
- **`net start crmdmgtd`** (on Windows)

Running the Hostname Change Script

You can either:

- Run the hostname change script without specifying any command line options

  After you have restarted your system, ensure that you stop the Daemon Manager and then enter the following command to run the hostname change CLI utility.

  – *NMSROOT*`\bin\perl` *NMSROOT*`\bin\hostnamechange.pl` (on Windows)

  – *NMSROOT*`/bin/perl` *NMSROOT*`/bin/hostnamechange.pl` (on Solaris/Soft Appliance)

Or

- Run the hostname change script with command line options

  Use this option to change the hostname only if the previous attempt of running this script had failed and the hostname changes were unsuccessful.

  You need not restart your machine to run the hostnamechange.pl CLI utility with command line options

  Enter the following command to run the `hostnamechange.pl` CLI utility:

  – *NMSROOT*`\bin\perl` *NMSROOT*`\bin\hostnamechange.pl -ohost` *Old_ Hostname* `-nhost` *New_Hostname* `-domain` *Domain* (on Windows)

  – *NMSROOT*`/bin/perl` *NMSROOT*`/bin/hostnamechange.pl -ohost` *Old_Hostname* `-nhost` *New_Hostname* `-domain` *Domain* (on Solaris/Soft Appliance)

  where,

  Old_ Hostname —Old Hostname of the LMS Server

  New_Hostname —New Hostname of the LMS Server

  Domain —Domain name of the LMS Server. Entering domain name is optional.

The `hostnamechange.pl` script performs the following:

1. Updates the new hostname of LMS Server in the following files:
   – /opt/CSCOpx/lib/classpath/md.properties (on Solaris/Soft Appliance)
   – /var/sadm/pkg/CSCOmd/pkginfo (on Solaris)
   – *NMSROOT*\lib\classpath\md.properties (on Windows)
2. Changes *ASName* to the new hostname of LMS Server in the following files:
   – /opt/CSCOpx/lib/classpath/sso.properties (on Solaris/Soft Appliance)
   – *NMSROOT*\lib\classpath\sso.properties (on Windows)
3. Updates the hostname in the following registry entry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager\CurrentVersion\Environment

   The CLI utility looks for all the instances of hostname under these registry entries, and replaces them with the new hostname.
4. Changes the hostname in regdaemon.xml (*NMSROOT*/MDC/etc/regdaemon.xml).
5. Changes the hostname in web.xml (*NMSROOT*/MDC/tomcat/webapps/classic/WEB-INF/web.xml).

6. Creates a file *NMSROOT*/conf/cmic/changehostname.info, with the information on the updated hostname in the format:

   OldhostName:*NewhostName*

   OldhostName—Previous hostname as registered with CCR(regdaemon.xml)

   NewhostName—Current hostname as registered with CCR(regdaemon.xml)

   The entries for hostname in regdaemon.xml and changehostname.info should be identical.

   The changehostname.info file resides in the LMS Server until you restart the Daemon Manager. This file will not be available in LMS Server after the Daemon Manager is restarted.

7. Deletes NS_Ref file on the following directories:
   - *NMSROOT*\lib\csorb (on Windows)
   - /opt/CSCOpx/lib/csorb (on Solaris/Soft Appliance)

   The NS_Ref file is restored in LMS Server after the Daemon Manager is restarted.

8. Starts the LMS 4.0 database and updates the database table entries with the new hostname. After updating the database table entries, it stops the LMS 4.0 database.

9. Detects and displays the details of the certificate in the LMS Server.
   - If the certificate is a third party certificate, you should regenerate your certificate with the new hostname.

   Or

   - If the certificate is a self-signed certificate, the script allows you to regenerate the certificate. You can enter **`y`** to re-generate the certificate with the new hostname or **`n`** to re-generate the certificate later. See Creating Self Signed Certificates for details.

After you have completed running the script, ensure that you:

- Start the Daemon Manager by entering the following commands:
  - **`/etc/init.d/dmgtd start`** (on Solaris/Soft Appliance)
  - **`net start crmdmgtd`** (on Windows)
- Redo the integration, if you have integrated any third party network management application to Cisco Prime, using Integration Utility.
- Re-import the certificates and redo the Multi-Server setup if the machine is part of a Multi-Server setup.

  For example, if you are changing the hostname of a machine that is configured as a Slave, then it needs to reregister with the Master. If you are changing the hostname of a machine that is configured as a Master, then all its Slaves need to be updated with the new Master hostname.

If the hostname of the machine changes, the stability of the system is not guaranteed and it fails in some cases.

Using DCR Features Through CLI

Using Command Line Interface, you can add, delete, and modify devices, and change the DCR modes. You can also view the list of attributes that can be stored in DCR, and view the current DCR mode. The **dcrcli** provided with LMS helps you perform these tasks using CLI.

The Device Name and the Host Name/Domain Name combination must be unique for each device in DCR. A device will be considered duplicate if:

- The Device Name of a device is the same as that of any other device
- The Host Name/Domain Name combination of a device is the same as that of any other device
- Auto Update Device ID is the same as that of any other device (in case of AUS managed device)
- Cluster and Member Number, together is same as that of any other device (in case of Cluster managed device)

dcrcli operates in both the Shell and Batch modes. The Shell mode is interactive whereas the Batch mode runs the specified command and exits to the prompt after the command is run.

You can set DCRCLIFILE environment to point to the file where LMS password is present. If you set DCRCLIFILE variable, password will not be asked when you run **dcrcli** in shell or batch mode.

The password file should contain an entry in the format *username password*. Make sure that there is only one blank space between the username and the password in the password file. For example, if admin is the username and the password for the Cisco Prime user, the password file must contain the following entry:

```
admin admin
```

This section has the following:

- Viewing the Current DCR Mode Using CLI
- Viewing Device Details
- Changing DCR Mode Using CLI

Viewing the Current DCR Mode Using CLI

To view the current DCR mode in Shell mode:

Step 1 Enter *NMSROOT*`/bin/dcrcli -u` *username*.

Step 2 Enter the password corresponding to the username.

Step 3 Enter `lsmode`

It lists the DCR ID, the DCR Group ID, the current DCR mode, and the associated Master and Slaves.

To view the current DCR mode in Batch mode:

Step 1 Go to *NMSROOT*`/bin`

Step 2 Enter `dcrcli -u` *Username* `cmd=`*lsmode*

Viewing Device Details

To view device details using **dcrcli** in Shell mode:

Step 1 Enter *NMSROOT*`/bin/dcrcli -u` *username*.

Step 2 Enter the password corresponding to the username.

Step 3 Enter `details id=`*DeviceID*

This lists all the details about the device with the ID you have specified. For example, `detail id=54341` lists the details for the device with device ID 54341.

To view device details using **dcrcli** in Batch mode:

Step 1 Go to *NMSROOT*`/bin`

Step 2 Enter `dcrcli -u` *Username* `cmd=`*detail* `id=`*DeviceID*

Changing DCR Mode Using CLI

To change mode to Master in Shell mode:

Step 1 Enter *NMSROOT*`/bin/dcrcli -u` *username*.

Step 2 Enter the password corresponding to the username

Step 3 Enter `setmaster`

The DCR mode gets changed to Master.

To change mode to Master in Batch mode:

Step 1 Go to *NMSROOT*`/bin`

Step 2 Enter `dcrcli -u` *Username* `cmd=setmaster`

To change mode to Standalone in Shell mode:

Step 1 Enter *NMSROOT*`/bin/dcrcli -u` *username*.

Step 2 Enter the password corresponding to the username

Step 3 Enter `setstand`

The DCR mode gets changed to Standalone.

To change mode to Standalone in Batch mode:

Step 1 Go to *NMSROOT*`/bin`

Step 2 Enter `dcrcli -u` Username `cmd=setstand`

To change mode to Slave in Shell mode:

Step 1 Enter *NMSROOT*`/bin/dcrcli -u` *username*.

Step 2 Enter the password corresponding to the username

Step 3 Enter `setslave master=`*value*

You have to specify the Master for this slave.

The DCR mode gets changed to Slave. For example,

```
setslave master=1.2.1.3 port=443
```

To change mode to Slave in Batch mode:

Step 1 Go to *NMSROOT*`/bin`

Step 2 Enter `dcrcli -u` Username `cmd=setslave master=`value

Using Group Administration Features Through CLI

You can use OGSCli command line utility to:

- Export Groups to an output XML file
- Import Groups to Grouping Server from an input XML file

You should have Network Administrator, System Administrator, or Super Admin privileges to use OGSCli command line utility.

OGSCli runs in only Batch mode. It runs the specified command and exits to the prompt after the command is run.

This section explains:

- Exporting Groups Through CLI
- Importing Groups Through CLI

Exporting Groups Through CLI

To export groups through CLI:

Step 1 Go to the command prompt.

Step 2 Enter either one of the following:

- *NMSROOT*`/bin/OGSCli.sh -u` *CiscoPrime_Username (on Solaris/Soft Appliance)*

Or

- *NMSROOT*`\bin\OGSCli -u` *CiscoPrime_Username (on Windows)*

where,

NMSROOT is the directory where you have installed Cisco Prime.

CiscoPrime_Username is the login username of a Cisco Prime user.

For example, you can enter `/opt/CSCOpx/bin/OGSCli.sh -u admin` on Solaris/Soft Appliance systems.

The system prompts you to enter your Cisco Prime password.

Step 3 Enter your Cisco Prime password.

The system prompts you to enter a task name, `import` or `export`. The default task is `export`.

Step 4 Enter `export`.

The system prompts you to enter an output file name.

Step 5 Enter a file name for export output file with its absolute path name.

If you do not enter file name with its absolute path name, the export file will be stored on \nmsroot\bin.

A warning message appears indicating that the selected file will be overwritten with the new information on exported groups.

The system uses the file name that you have entered to generate the output XML file irrespective of whether the file exists on the server.

You should have the required directory-level permissions where you want to save the output XML file.

You must either enter `y` to continue or `n` to exit.

The system prompts you to enter an export group hierarchy.

Step 6 Enter `All` or the export group hierarchy name.

Default value is `All`.

For example, you can enter the group hierarchy name as `/CS@doc-pc2/User Defined Groups/Group1`.

The system generates an export format XML file and stores on the specified directory on the server.

Importing Groups Through CLI

To import groups through CLI:

Step 1 Go to the command prompt.

Step 2 Enter either one of the following:

- *NMSROOT*`/bin/OGSCli.sh -u` *CiscoPrime_Username (on Solaris/Soft Appliance)*

Or

- *NMSROOT*`\bin\OGSCli -u` *CiscoPrime_Username (on Windows)*

where,

NMSROOT is the directory where you have installed Cisco Prime.

CiscoPrime_Username is the login username of a Cisco Prime user.

For example, you can enter `/opt/CSCOpx/bin/OGSCli.sh -u admin` on Solaris/Soft Appliance systems.

The system prompts you to enter your Cisco Prime password.

Step 3 Enter your Cisco Prime password.

The system prompts you to enter a task name, import or export. The default task is export.

Step 4 Enter `import`.

The system prompts you to enter the input XML filename.

Step 5 Enter the input XML filename with its absolute path name.

The system lists the groups to be imported from the source XML file.

Step 6 Enter your choices using the item numbers displayed for the listed groups.

You can enter one or more item numbers separated by comma.

The system lists the Grouping Server locations where you can import the groups.

Step 7 Enter your choices using the item numbers displayed for the listed Grouping Servers.

You can enter one or more item numbers separated by comma. You must enter `1` to import the selected groups to all listed servers.

A message appears indicating whether the import of groups is successful.

See Exporting Groups for the possible causes for the import groups job to fail.

Deleting Stale Groups Using CLI

You can delete groups that belonged to users removed from Cisco Prime. To delete a stale group, you must run the DeleteStaleGroups utility.

To run the DeleteStaleGroups utility:

On Windows:

Step 1 Enter *NMSROOT*`\bin`

Step 2 Enter `DeleteStaleGroups -user` *username* `-pfile` *passwordfile* `-staleuser` *StaleUser*

On Solaris/Soft Appliance:

Step 1 Enter *NMSROOT*`/bin`

Step 2 Enter `DeleteStaleGroups.sh -user` *username* `-pfile` *passwordfile* `-staleuser` *StaleUser*

The explanation for these optional entries are as follows:

`-user`: Current user who has the necessary privileges to delete groups.

`-pfile`: Absolute Path of the text file with Cisco Prime login password of the current user, in one line.

`-staleuser`: The user whose group has to be deleted.

If you run the DeleteStaleGroups utility without specifying any of these optional entries, all the stale groups will be deleted.

User Tracking Command Line Interface

You can run User Tracking commands from the command line in Solaris/Soft Appliance and Windows 2000.

Enter `ut -cli` *options* `-u` *username* `-p` *password*.

The *options* can be one or more of those shown in Table A-1.

- Use the `-prompt` command if you do not want to enter your password from the command line. Using `-prompt` prevents other users from running `ps` and seeing your password.
- The `-host` option is required when you run the CLI command on a remote LMS Server.

Table A-1 User Tracking CLI Commands

Option	Arguments	Function
`-prompt`	No keywords or arguments.	This command is required if you do not enter your password from the command line. If -**prompt** is specified, User Tracking prompts you to enter your password.
`-help`	No keywords or arguments.	Prints the command line usage.
`-ping`	*{enable | disable}*	Enables the Ping Sweep option so that the ANI Server pings every IP address on known subnets before discovery. The default is the last setting used. User Tracking does not perform Ping Sweep on large subnets, for example, subnets containing Class A and B addresses. Hence, ARP cache might not have some IP addresses and User Tracking may not display the IP addresses. In larger subnets, the ping process leads to numerous ping responses that might increase the traffic on your network and result in extensive use of network resources. To perform Ping Sweep on larger subnets, you can: • Configure a higher value for the ARP cache time-out on the routers. To configure the value, you must use the **`arp time-out interface configuration`** command on devices running Cisco IOS. • Use any external software, which will enable you to ping the host IP addresses. This ensures that when you run User Tracking Acquisition, the ARP cache of the router contains the IP addresses.
`-performMajorAcquisition`	No keywords or arguments.	Acquires data about all users and hosts on the network and updates the LMS database. This option starts an acquisition but does not wait for it to complete.

Table A-1 User Tracking CLI Commands (continued)

Option	Arguments	Function
`-query`	This option takes one of the following arguments:	Queries the Topology and Layer 2 services module database and updates the User Tracking table.
	all	Gets all User Tracking entries. Similar to “All Host Entries” or a simple query in the GUI.
	name	Runs the named advanced or simple query, created earlier in the GUI.
	dupMAC	Finds duplicate MAC addresses.
	dupIP	Finds duplicate IP addresses.
	hub	Finds ports with multiple MAC addresses (hubs).
`-queryPhone`	*all*	Gets all IP Phone entries.
	name	Runs the named advanced query, created earlier in the GUI.
`-layout`	*layout_name*	Uses the specified main table layout while performing a query to fetch User Tracking display entries.
`-layoutPhone`	*layout_name*	Uses the specified IP phone table layout while performing a query to fetch IP phone display entries.
`-host`	*ANI Server device name or IP Address*	Specifies the host name or IP address of the LMS Server. Use this argument when you need to run the CLI command on a remote LMS Server.
`-port`	*ANI Server web port number*	Specifies the web server port number of the ANI Server. The default is 1741.
`-export`	*filename*	Exports data to a text file. You must first specify the `-query` option to fetch the data that you want to export.
`-import`	*filename*	Imports lost or deleted UserName and Notes fields from the last exported file.
-importMACToAcceptableOUI	filename	Imports MACs and converts them to OUI and adds the MACs to the Acceptable OUI List. For example: `cd NMSROOT/bin ut -cli -importMACToAcceptableOUI filename -u username -p password`
`-stat`	No keywords or arguments.	Displays statistical information, such as time of last acquisition, acquisition status, number of records in the User Tracking database, and so on.
`-debug`	No keywords or arguments.	Enables trace and debug messages for the User Tracking client application.

Table A-1 User Tracking CLI Commands (continued)

Option	Arguments	Function
`-wireless`	No keywords or arguments.	Displays detailed information on Wireless clients connected to the network. If you enter this option along with the **export** option, data can be exported to a text file. For example: ***NMSROOT*/campus/bin ut -cli -wireless -export *c:/sample* -u *username* -p *password***
`-switchPortCapacity`	For complete details on this, see Exporting Switch Port Usage Report.	
`-switchPortreclaimreport`	For complete details on this, see Exporting Switch Port Usage Report	
`-switchPortSummary`	For complete details on this, see Exporting Switch Port Usage Report	

For details on Lookup Analyzer Script, see Using Lookup Analyzer Utility

Exporting Switch Port Usage Report

Switch Port Capacity report lists switches whose utilization percentage falls in the specified range.

Switch Port Reclaim reports lists:

- Ports that are administratively up or down

  and

- Ports that were previously connected to an endhost or a device but are unconnected at least for a period of one day.

Switch port usage reports can be generated from the command prompt as given in Table A-2:

Table A-2 Switch Port Reports from the Command Prompt

Purpose	Command
Switch Port Capacity Report	
To generate reports where the utilization is less than the specified percentage (for all devices managed by LMS)	*NMSROOT*`/campus/bin ut -cli -switchPortCapacity lessthan` *60* `-devices all -export` *c:/sample* `-u` *username* `-p` *password*
To generate reports where the utilization is less than the specified percentage (for specific devices)	*NMSROOT*`/campus/bin ut -cli -switchPortCapacity lessthan` *60* `-devices` *10.77.2.1,10.77.3.4,10.77.5.6* `-export` *c:/sample* `-u` *username* `-p` *password*
To generate reports where the utilization is greater than the specified percentage (for all devices managed by LMS)	*NMSROOT*`/campus/bin ut -cli -switchPortCapacity greaterthan` *60* `-devices all -export` *c:/sample* `-u` *username* `-p` *password*
To generate reports where the utilization is greater than the specified percentage (for specific devices)	*NMSROOT*`/campus/bin ut -cli -switchPortCapacity greaterthan` *60* `-devices` *10.77.2.1,10.77.3.4,10.77.5.6* `-export c:/sample -u` *username* `-p` *password*
To generate reports where the utilization falls between the specified range (for all devices managed by LMS)	*NMSROOT*`/campus/bin ut -cli -switchPortCapacity between` *10 60* `-devices all -export` *c:/sample* `-u` *username* `-p` *password*
To generate reports where the utilization falls between the specified range (for specific devices)	*NMSROOT*`/campus/bin ut -cli -switchPortCapacity between` *10 60* `-devices` *10.77.2.1,10.77.3.4,10.77.5.6* `-export` *c:/sample* `-u` *username* `-p` *password*

Table A-2 Switch Port Reports from the Command Prompt

Purpose	Command
Switch Port Reclaim Report	Generates reports for unused ports that are in up or down state.
To generate Reclaim Unused Up Ports report (for all devices managed by LMS)	*NMSROOT*/campus/bin ut -cli -switchPortReclaimReport type *up* days *2* -devices all -export *c:/sample* -u *username* -p *password*
To generate Reclaim Unused Up Ports report (for specific devices)	*NMSROOT*/campus/bin ut -cli -switchPortReclaimReport type *up* days *2* -devices *10.77.1.2,10.77.3.4* -export *c:/sample* -u *username* -p *password*
To generate Reclaim Unused Down Ports report (for all devices managed by LMS)	*NMSROOT*/campus/bin ut -cli -switchPortReclaimReport type *down* days *2* -devices all -export *c:/sample* -u *username* -p *password*
To generate Reclaim Unused Down Ports report (for specific devices)	*NMSROOT*/campus/bin ut -cli -switchPortReclaimReport type *down* days *2* -devices *10.77.1.2,10.77.3.4* -export *c:/sample* -u *username* -p *password*
Switch Port Summary Report	Generates reports that gives the number of Connected, Free, and Free down ports in each switch.
To generate Switch Port Summary report for all devices	*NMSROOT*/campus/bin ut -cli -switchPortSummary -devices all -export *c:/sample* -u *username* -p *password*
To generate Switch Port Summary report for select devices	*NMSROOT*/campus/bin ut -cli -switchPortSummary -devices *10.77.1.2,10.77.3.4* -export *c:/sample* -u *username* -p *password*

where ***NMSROOT*** is the directory where you installed Cisco Prime.

Note The above commands can be run in a Solaris/Soft Appliance machine. To run the same commands in Windows, replace all forward slash (/) with reverse slash (\).

The report generated by the above options is saved as a file in the CSV format, at the specified location.

You can generate various Switch Port Usage reports, select **Reports > Switch Port**.

Using Lookup Analyzer Utility

Lookup Analyzer is a utility used to analyze the performance of DNS servers and provide the following information:

- DNS Server Efficiency for each DNS Server
- Overall Summary of DNS Servers

- Namelookup related settings in ut.properties file
- Issues found and recommendations to overcome them

For Solaris/Soft Appliance:

The utility file is *NMSROOT*/campus/bin/LookupAnalyzer.sh

If dir is the directory where the file is present, run the following command to run the utility:

dir# **`./LookupAnalyzer`**

For Windows:

The utility file is *NMSROOT*\campus\bin\LookupAnalyzer.bat

If dir is the directory where the file is present, run the following command to run the utility:

dir> **`LookupAnalyzer`**

Example output of the Lookup Analyzer script:

```
Host IP: 172.20.123.74, DNS Server: 64.104.76.247, Time taken: 35, Status: FAILURE
Host IP: 172.20.123.74, DNS Server: WINS, Time taken: 22, Status: FAILURE
Host IP: 10.77.209.254, DNS Server: 64.104.128.248, Time taken: 18, Status: FAILURE
..
..
DNS Server   : 64.104.128.248
Success Count: 12
Failure Count: 76
Failure %    : 86 %
Total Time   : 1 secs 561 ms
Min Time     : 0 ms
Max Time     : 52 ms
Avg Time     : 17 ms
Server Efficiency(successCount/totalTime): 7.0
--------------------------------
DNS Server   : 64.104.76.247
Success Count: 0
Failure Count: 76
Failure %    : 100 %
Total Time   : 2 secs 729 ms
Min Time     : 0 ms
Max Time     : 61 ms
Avg Time     : 35 ms
Server Efficiency(successCount/totalTime): 0.0
--------------------------------
DNS Server   : WINS
Success Count: 0
Failure Count: 76
Failure %    : 100 %
Total Time   : 750 ms
Min Time     : 0 ms
Max Time     : 23 ms
Avg Time     : 9 ms
Server Efficiency(successCount/totalTime): 0.0
--------------------------------
Overall Summary
-----------------
Success Count: 12
Failure Count: 76
Failure %    : 86 %
-----------------
Current Namelookup Related Settings
---------------------------------
UTMajorUseDNSSeperateThread: false
UT.nameResolution: both
UT.nameResolution.threadCount: 1
UT.nameResolution.winsTimeout: 2000
UT.nameResolution.threadThresholdPercentage: 10
UT.nameResolution.dnsTimeout: 2000
UTMajorUseDNSCache: false
nameserver.usednsForUT: true
DB.dsn: ani
---------------------------------
ISSUES/RECOMMENDATIONS
-----------------------
Issue #1: Failure Percent is greater than 20%
Recommendation: Check all DNS/WINS entries and ensure proper hostnames are configured

Issue #2: DNS reverse lookup is NOT done as separate process
Recommendation: Enable UTMajorUseDNSSeperateThread=true in ut.properties

Issue #3: Name Resolution DNS server order is not optimal
Recommendation: Change dns server order as 64.104.128.248=7.0, 64.104.76.247=0.0,
WINS=0.0,

Other Recommendations:
* If hostnames in your network are less likely to change often, set
UTMajorUseDNSCache=true
* If reverse lookup failure % is more, try increasing UT.nameResolution.winsTimeout,
UT.nameResolution.dnsTimeout and UT.nameResolution.threadThresholdPercentage
* Optimal timeout values are: UT.nameResolution.winsTimeout=0,
UT.nameResolution.dnsTimeout=48
```

The script can also be run by setting properties in the ut.properties file.

Understanding UTLite

UTLite is a utility that allows you to collect user names from Primary Domain Controllers, Active Directory, and Novell servers.

To do this you need to install UTLite in the Windows Primary Domain Controllers and in the Novell servers. You can also install UTLite in an Active Directory server.

UTLite sends traps to LMS whenever a user logs in or logs out. UTLite traps are processed by LMS at the rate of 150 traps per second, with a default buffer size of 76800.

If you need a higher trap processing rate, say 300 traps per second, increase the buffer size to 102400.

To increase the buffer size:

Step 1 Enter **`pdterm UTLITE`** at the command line to stop the UTLite process.

Step 2 Open utliteuhic.properties located at *NMSROOT*\campus\lib\classpath\com\cisco\nm\cm\ut\uhic\utlite\properties\

Step 3 Set Socket.portbuffersize=102400

Step 4 Enter **`pdexec UTLITE`** at the command line to start the UTLite process.

Caution Increasing the buffer size beyond 102400 results in performance degradation of UTLite.

To receive UTLITE events:

Step 1 Open utliteuhic.properties located at *NMSROOT*\campus\lib\classpath\com\cisco\nm\cm\ut\uhic\utlite\properties\

Step 2 Change the property of URTlite state by changing the value from "URTlite.state=disable" to "URTlite.state=enable".

Or

You can change the property of URTlite state by launching LMS. Select the Acquisition Settings option from **Admin > Collection Settings > User Tracking > Acquisition Settings**. The Acquisition Settings page appears. In the Acquisition Settings page, check the Get user names from hosts in NT and NDS domains and click **Apply**.

Note The servers should be DNS resolvable to get the events from the clients. Else we have to make entry in %WINDIR%\system32\drivers\etc\hosts.

The UTLite script is **supported** on these platforms:

- Windows NT
- Windows 2000
- Windows XP
- Windows 2003
- Windows Vista
- Novell Directory Services (NDS)
- Windows 7 (Client OS support)

The UTLite script is **not supported** on these UNIX hosts:

- Solaris
- HP-UX
- AIX

This section contains:

- Installing UTLite Script on Active Directory/Windows
- Installing UTLite Script on NDS
- Uninstalling UTLite Scripts From Windows
- Uninstalling UTLite Scripts From Active Directory
- Uninstalling UTLite Scripts From NDS

Installing UTLite Script on Active Directory/Windows

You must install the UTLite script on the Active Directory server and update the server’s logon script to get user logon information from Active Directory hosts.

You must have Administrator privileges on the Active Directory server to install the UTLite logon script. To install the script:

Step 1 Copy the required files to the Active Directory server:

a. Log into the Active Directory server as Administrator.

b. Obtain the UTLite files from the Server Configuration:

NMSROOT`\campus\bin\UTLite33.exe`

NMSROOT`\campus\bin\UTLiteNT.bat`

where *NMSROOT* is the directory in which you installed Cisco Prime.

c. Copy the UTLiteNT.bat and UTLite33.exe files into the NETLOGON folder.

NETLOGON is located at:
%SystemRoot%\sysvol\sysvol\domain DNS name\scripts,

where %SystemRoot% is usually *c:\winnt* and *domain DNS name* is the DNS name of the domain

Note For Windows 2000 and NT servers, the NETLOGON folder is located at: *%SYSTEMROOT%\system32\Repl\Import\Scripts*

Step 2 Edit the UTLiteNT.bat file:

a. Open the UTLiteNT.bat file.

b. Locate the following line and replace *domain* and *ipaddress* with the domain name of the Windows domain controller and IP address of the computer running the Campus Manager server:

`start` *%WINDIR%*`\UTLite33 -domain` *domain* `-host` *ipaddress* `-port 16236`

For example:

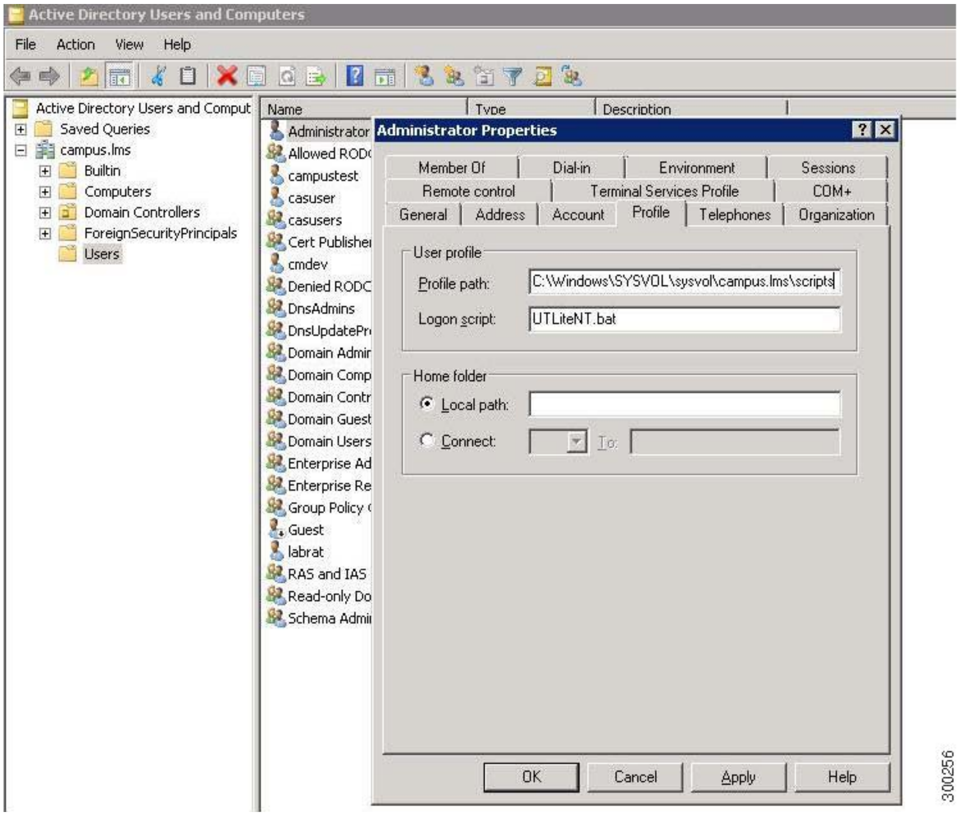
start %WINDIR%\UTLite33 -domain cdiclab.cisco -host 192.168.152.228 -port 16236

If port 16236 is already in use, enter a different number. This port number must match the number that you entered in the Use Port Number field, in the User Tracking Acquisition Settings page (Select **Admin > Collection Settings > User Tracking > Acquisition Settings**).

For more details, see Modifying UT Acquisition Settings.

Step 3 Edit the user profile on the Active Directory server to run the UTLiteNT.bat file when users log in to the network by editing the profile of the user as shown in Figure A-1:

Figure A-1 Active Directory User Profile



Profile path: C:\Windows\SYSVOL\sysvol\campus.lms\scripts

Logon script: UTLiteNT.bat

● Local path:

○ Connect:

Here, in the User profile section of the window, the Profile path is set to be:

C:\windows\sysvol\sysvol\domain\scripts

The Logon script is set to be:

`UTLiteNT.bat`

Step 4 Update the domain controller logon script for each Windows domain that you add.

The first time users log into the network after you edit this script, UTLite33.exe is copied to the local WINDIR directory on their Windows client system.

Installing UTLite Script on NDS

You must install the UTLite script on the Novell Server and update the domain controller logon script, to get user logon information from Windows hosts. You only need to do this once for each domain.

You must have ZenWorks installed and running on the Novell Server, and you must be using NDS 5.0 or later.

To install the script:

Step 1 Copy the required files to the Novell Server.

Step 2 Log into the Novell Server as Administrator.

Step 3 Obtain the UTLite files from the LMS Server:

- *NMSROOT*`\campus\bin\UTLite33.exe`
- *NMSROOT*`\campus\bin\UTLiteNDS.bat`

  where *NMSROOT* is the directory in which you installed Cisco Prime.

Step 4 Create a folder in \\Novell Server Name\SYS\public and copy UTLiteNDS.bat and UTlite33.exe to the folder.

Step 5 Edit the UTLiteNDS.bat file:

Step 6 Open the UTLiteNDS.bat file.

Step 7 Locate the following line and replace *domain* and *ipaddress* with the domain name of the Windows domain controller and IP address of the computer running the LMS server:

`start` *%WINDIR%*`\UTLite33 -domain` *domain* `-host` *ipaddress* `-port 16236`

If port 16236 is already in use, enter a different number. This port number must match the number that you entered in the Use Port Number field, in the User Tracking Acquisition Settings page (Select **Admin > Collection Settings > User Tracking > Acquisition Settings**).

For more details, see Modifying UT Acquisition Settings.

Edit the logon scripts.

Step 8 Enter \\Novell_Server_Name`\SYS\public\NaL.exe` at the command prompt.

Step 9 Click **NWAdmin32** to run the Novell Netware Administrator program.

Step 10 Right-click on the users or organizational units whose logon scripts you want to modify and select Details.

Step 11 Click **Login Script** and enter:

@\\*%FILE_SERVER%*`\sys\public\`*your_folder_name*`\UTLiteNDS.bat` where *your_folder_name* is the name of the folder you created in Step 1.

Uninstalling UTLite Scripts From Windows

If you choose not to have LMS server automatically collect user names, follow these instructions to properly remove the UTLite scripts. To uninstall the script:

Step 1 Remove UTLiteNT.bat and UTLite33.exe files from each primary domain controller.

Step 2 Remove the call to run UTliteNT.bat from users' logon scripts.

Step 3 Delete UTLite33.exe from the *WINDIR* directory of all Windows clients.

To quickly locate the *WINDIR* directory, enter `set windir` from a command prompt window on each client.

Uninstalling UTLite Scripts From Active Directory

If you choose not to have LMS server automatically collect user names, follow these instructions to properly remove the UTLite scripts. To uninstall the script:

Step 1 Remove UTLiteNT.bat and UTLite33.exe files from each Active Directory server.

Step 2 Remove the call to run UTliteNT.bat from users' logon scripts.

Step 3 Delete UTLite33.exe from the *WINDIR* directory of all Windows clients.

To quickly locate the *WINDIR* directory, enter **`set windir`** from a command prompt window on each client.

Uninstalling UTLite Scripts From NDS

If you choose not to have LMS server automatically collect user names, you must perform these steps to properly remove the UTLite scripts. To uninstall the script:

Step 1 Remove UTLiteNDS.bat and UTLite33.exe files from the Novell Server.

Step 2 Remove the line added to the login scripts for all users and organizational units.

Step 3 Delete UTLite33.exe from the *WINDIR* directory of all clients.

To quickly locate the *WINDIR* directory, enter **`set windir`** from a command prompt window on each client.

User Tracking Debugger Utility

The User Tracking Debugger Utility is a command line tool to help debug common problems with User Tracking. This section contains:

- Understanding Debugger Utility
- Using Debugger Utility

Understanding Debugger Utility

The utility displays a report on the reasons why User Tracking failed to discover end hosts on specific ports.

In many cases, User Tracking may not perform as expected. This may be because of problems in other LMS applications. For instance LMS Server may have devices that are not discovered or inadequate VLAN discovery in Topology Services.

You can run the utility to troubleshoot problems, or provide the report and log generated by the utility when you contact TAC for help in diagnosing problems.

The debugger utility uses the data collected by LMS Server and reports the reasons for the missing ports in User Tracking.

This tool also has an SNMP component embedded which runs an SNMP query for the table as a part of verification for SNMP failure. For example, SNMP bugs in Catalyst operating system because of which User Tracking may fail to discover devices.

This generates an Action Report that you can use to analyze the data.

The Debugger Utility:

1. Checks the switch ports in a sequential order.
2. Reports violation of basic rules for each of the missing ports such as link ports and trunk ports.
3. Checks for SNMP retrieval of data, if the ports pass the validity check.
4. Generates an Action Report suggesting possible remedial actions to retrieve the valid missing ports.

Using Debugger Utility

The Debugger Utility is available at *$NMSROOT*/campus/bin/ (where *$NMSROOT* is the directory where you have installed Cisco Prime).

To run the Debugger Utility, run the command:

utdebug -switch *switch-ip* **-port** *port1[,port2 ...]* [**-export** *filename*]

where,

switch is the switch to which the end hosts are connected.

ports are the ports on the switch which have missing end hosts User Tracking.

-export *filename* specifies that the debug messages be stored in the file specified. If this option is not used, the messages are displayed on the console.

```
For example,
utdebug -switch 10.29.6.12 -port 5/12
utdebug -switch 10.29.100.10 -port Fa0/10
utdebug -switch 10.29.6.14 -port Gi6
```

Configuring Switches to Send MAC Notifications to LMS Server

You must configure the Cisco switches for sending SNMPv1/SNMPv2 MAC Notification Traps when a host is connected to or disconnected from that port. Even if the device is managed with SNMPv3, Network Topology, Layer-2 Services, and User Tracking, it processes only SNMPv1/SNMPv2 traps.

You can configure the ports only through Command Line Interface (CLI). If you do not have Configuration Management functionality enabled on your LMS Server, you have to manually configure the switches for the switches to send MAC Notifications to the LMS server. Ensure that you have configured System Identity User under **Admin > Trust Management > Multi Server > System Identity Setup** and the same username and password is configured under **Admin > System > User Management > Local User Setup**.

For a list of commands to be run on each device, see the Appendix Commands to Enable MAC Notification Traps on Devices.

For complete list of devices supported by LMS, see http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.2/device_support/table/lms42sdt.html

Administration Command Line Interface

This section describes how to administer LMS database from the command line. This is explained in the following topics:

- Replacing Corrupted Database
- Re-initializing the Database
- Deleting all Active Entries from User Tracking, and Restarting Servers
- Deleting all Inactive Entries from User Tracking, and Restarting Servers
- Deleting all History Entries from User Tracking, and Restarting Servers
- Deleting all User Tracking Entries, and Restarting Servers
- Restoring the Original Data in the Server
- Restoring Data from Another Server
- Performance Tuning Tool

This section also explains SNMP Configuration on Devices

Replacing Corrupted Database

If you have a corrupted database, you can use the database administration tools to restore the database from a previous backup. However, if you do not have a previous backup, you must re-initialize the database.

When you run this command, if Data Collection is running, it is automatically stopped and then restarted when the database initialization is complete.

Caution If you re-initialize the database, information from discovered devices will be lost. However, user and host information is retained. Replace the database only if recommended by a Cisco technical representative.

Note Your login determines whether you can use this option.

Re-initializing the Database

From the command prompt or shell window, enter:

- On Solaris/Soft Appliance: *NMSROOT*`/campus/bin/reinitdb.pl`
- On Windows: `perl` *NMSROOT*`\campus\bin\reinitdb.pl`

  The following message appears:

  ```
  This will erase all data from the database. Are you sure [y/n] ?
  ```

  If you enter **y**, it erases all data (database tables Wbu*...) from the server.

Deleting all Active Entries from User Tracking, and Restarting Servers

From the command prompt or shell window, enter:

- On Solaris/Soft Appliance: *NMSROOT*`/campus/bin/reinitdb.pl -ut -active`
- On Windows: `perl` *NMSROOT*`\campus\bin\reinitdb.pl -ut -active`

where active entries are hosts that are currently logged in

Deleting all Inactive Entries from User Tracking, and Restarting Servers

From the command prompt or shell window, enter:

- On Solaris/Soft Appliance: *NMSROOT*`/campus/bin/reinitdb.pl -ut -inactive`
- On Windows: `perl` *NMSROOT*`\campus\bin\reinitdb.pl -ut -inactive`

where inactive entries are hosts that are currently not logged in

Deleting all History Entries from User Tracking, and Restarting Servers

From the command prompt or shell window, enter:

- On Solaris/Soft Appliance: *NMSROOT*`/campus/bin/reinitdb.pl -ut -history`
- On Windows: `perl` *NMSROOT*`\campus\bin\reinitdb.pl -ut -history`

where history entries are complete entries. That is, hosts that have a login and logout in the past.

Deleting all User Tracking Entries, and Restarting Servers

From the command prompt or shell window, enter:

- On Solaris/Soft Appliance: *NMSROOT*`/campus/bin/reinitdb.pl -ut -all`
- On Windows: `perl` *NMSROOT*`\campus\bin\reinitdb.pl -ut -all`

Restoring the Original Data in the Server

From the command prompt or shell window, enter:

- On Solaris/Soft Appliance: *NMSROOT*`/campus/bin/reinitdb.pl -restore`
- On Windows: `perl` *NMSROOT*`\campus\bin\reinitdb.pl -restore`

Note Before executing the `-restore` command, you should stop the daemon manager and start again manually. For details, see Using Daemon Manager.

Restoring Data from Another Server

When you take database backup for LMS in one server and restore it in another server, the *NMSROOT* logfile location may not be the same in both servers.

In that case, LMS will log messages to the log file stored in the default *NMSROOT* location in the restored machine.

where *NMSROOT* is the root directory where you installed Cisco Prime.

Performance Tuning Tool

When you get out of memory errors in LMS, the following command can be used to tune the performance:

NMSROOT`/bin/perl` *NMSROOT*`/campus/bin/CMPTT.pl` *ProcessName HeapSize MaxPermSize*

- ProcessName should be either one of the following:
  - ANIServer
  - UTMajorAcquisition
- Heap size should be multiples of 512 and should not exceed 1536 MB.

  Ensure you have enough swap space in the server before tuning the heap size.
- MaxPermSize will set the JVM MaxPermSize option to 64m.

SNMP Configuration on Devices

SNMP v3 Device Configuration Settings

LMS supports the following Authentication protocols for SNMP v3:

- md5
- SHA

LMS supports the following Privacy protocols for SNMP v3:

- des
- 3des
- aes128
- aes192
- aes256.

For using various LMS features in devices running SNMPv3, you must make specific configurations on the devices. The commands that need to be configured are:

- Configuring MIB Views
- Configuring Access Groups
- Configuring Device with Context Name
- Configuring a New User
- Configuring Password for a User
- Relating a User to a Group
- Configuring Privacy Protocol

Configuring MIB Views

For Catalyst devices, enter the following command:

```
set snmp view campusview 1.3.6.1 included nonvolatile
```

For IOS devices, enter the following command:

```
snmp-server view campusview oid-tree included
```

Configuring Access Groups

You must set the access rights for a group with a certain security model in different security levels.

For Catalyst devices, enter the following command:

```
set snmp access campusgroup security-model v3 authentication read campusview write
campusview nonvolatile
```

For IOS devices, enter the following command:

```
snmp-server group campusgroup v3 auth read campusview write campusview access access-list
```

Configuring Device with Context Name

For Catalyst devices, enter the following commands:

```
set snmp access campusgroup security-model v3 authentication read campusview write
campusview context vlan- prefix nonvolatile
```

Context exact is also supported. The following is an example:

```
set snmp access campusgroup security-model v3 authentication read campusview write
campusview context vlan-1 exact nonvolatile
```

For IOS devices, enter the following command:

```
snmp-server group campusgroup v3 auth context vlan-1 read campusview write campusview
```

IOS image versions prior to12.4 support only exact context name.

IOS image versions 12.4 or higher, support both *exact* or *prefix context names*.

You need to configure the device with and without context name, since Data Collection manages the device without context name and User Tracking requires context name to contact the device.

Configuring a New User

For Catalyst devices, enter the following command:

```
set snmp user campususer authentication md5
```

For IOS devices, enter the following command:

```
snmp-server user campususer campusgroup v3 auth md5 password1
```

Configuring Password for a User

For Catalyst devices, enter the following command:

```
set snmp user campususer authentication md5 password1
```

For IOS devices, enter the following command:

```
snmp-server user campususer campusgroup v3 auth md5 password1
```

Relating a User to a Group

Using a specified security model you can relate a user to a group.

For Catalyst devices, enter the following command:

```
set snmpw group campusgroup user campususer security-model v3 nonvolatile
```

For IOS devices, enter the following command:

```
snmp-server user campususer campusgroup v3
```

Configuring Privacy Protocol

For Catalyst devices:

```
set snmp user campususer authentication md5 password1privacy des password2
```

For IOS devices:

```
snmp-server user campususer campusgroup v3 auth md5 password1 priv des password2
```

Configuring SNMP view to prevent %SNMP-3-AUTHFAIL Syslog due to polling of shutdown VLANs

Due to the limitation of stpxPVSTVlanEnable mib object, data collection polls shut down VLANs for fetching STP related data which will enable the device to trigger %SNMP-3-AUTHFAIL Syslogs. In order to avoid the polling of shut down VLAN, SNMP-VACM-MIB view has to be created in the device, associated with SNMP credential and the property vacmContextNameEnabled has to be set to 1 in LMS.

You can enable it by creating a view and by including and excluding MIBs. To create a SNMP view:

Step 1 Create a SNMP view as follows in device x:

```
snmp-server view <view-name> iso included
snmp-server view <view-name> internet included
snmp-server view <view-name> internet.6.3.15 excluded
snmp-server view <view-name> w1 internet.6.3.16 excluded
snmp-server view <view-name> internet.6.3.18 excluded
snmp-server view <view-name> cTapMIB excluded
snmp-server view <view-name> internet.6.3.16.1.1 included
```

Step 2 Associate the view with SNMP v2 RO community string.

```
snmp-server community <community string> view <view-name> RO
```

Step 3 Shut down a vlan in device x.

Step 4 In ANIServer.properties, set vacmContextNameEnabled=1 and restart ANIServer.

Step 5 Run DC for device x.

Note During data collection LMS is quering vacmContextName variable of SNMP-VACAM-MIB. From this MIB variable LMS can find out which vlans are in shut down state so that LMS will try to connect to that vlan context. This MIB will be not supported by the device by default.

In LMS, by default the property vacmContextNameEnabled in ANIServer.properties under NMSROOT/campus/ect/cwsi has the value 0. This value has to be changed to 1 and then restart the daemons.

Note The device side configuration has to be done on all the devices in the network before changing the property in LMS. Otherwise some of the features will not work in Topology and Layer2 Services.