CHAPTER 7

User Tracking and Dynamic Updates

User Tracking application of LMS allows you to track end stations. This chapter contains the following sections:

Understanding User Tracking

User Tracking helps you to locate and track the end hosts in your network. In this way, you get the information required to troubleshoot and analyze connectivity issues. The application identifies all end users connected to the discovered Cisco access layer switches on the network, including printers, servers, IP phones PCs and wireless hosts.

User Tracking collects the details of the end users and the layer 2 connections, and updates User Tracking table in the LMS database. This is done through automated polling of the network, by User Tracking (UT) Major Acquisition process.

In addition to polling the network, the Dynamic UT process receives details from the end users and updates the database dynamically. User Tracking also computes subnet related data and updates the database with complete host information. Thus you get latest information about the changes in the connections on your network.

You can also configure User Tracking to collect usernames of the end hosts connected in the network. The user names are collected from the UTLite process installed in UNIX hosts, Primary Domain Controller (PDC), or Novell Directory Services (NDS). This makes it easier for you to locate and track specific users in your network.

You can sort and query the User Tracking table that contains details such as VLANs, switches and switch ports to which the end users are connected. Predefined reports such as the reports on duplicate IP addresses or MAC addresses, multiple MAC addresses enable you to accurately locate the end users.

Switch Port reports give you information on:

- Recently down ports
- Ports that are in unused condition for the specified interval
- Connected ports and Free ports
- Percentage utilization of ports for each device

These reports give a clear picture of the switch port utilization in the network and help you in doing capacity planning for the network. To generate Switch Port reports Select **Reports > Switch Port** from the megamenu.

This topic covers:

Using User Tracking

You can use User Tracking to:

- Display information about the connectivity between the devices, users, and hosts in your network. For example, you might want to identify all users connected to a particular subnet, or all hosts on a particular switch.
- Display information about the IP phones registered with discovered Media Convergence Servers.
- Use simple queries to limit the amount of information User Tracking displays.
- Configure or limit the User Tracking acquisition by subnets.
- Create and save simple and advanced queries.
- Modify, add, and delete username and notes.

  You can configure User Tracking Acquisition settings to collect usernames during UT Major Acquisition and update the UT table. The user names are collected from the UTLite process.
- Customize User Tracking table layouts.

  For example, you can design a layout that displays only the MAC addresses of hosts on your network.
- View User Tracking reports that identify Switch Port usage, duplicate IP addresses, duplicate MAC addresses, duplicate MAC and VLAN names, and ports with multiple MAC addresses.

  You can also view History Reports for Switch port utilization, and the connection and disconnection of endhosts and users from your network.

  You can set the schedule for generating the reports, and also generate the reports for a subset of devices.
- Launch Device Center, host center, phone center.

Accessing UT Data

The following are the ways to access User Tracking data:

Quick Reports

You can generate End hosts or IP Phones report based on the given filter criteria

For example, you can generate reports on end hosts that belong to a specific VLAN.

To generate these reports, Select **Reports > Inventory > User Tracking > Quick Report**.

Scheduled Reports

You can schedule reports that run at the specified date and time. You can generate immediate reports or schedule them to run once or at repetitive intervals.

Custom Reports

You can customize the layout and columns displayed in the reports to suit your needs. To generate these reports select **Reports > Report Designer > User Tracking > Custom Reports**.

Command Line Interface

You can generate various User Tracking reports from the Command Line Interface also.

For more details, see User Tracking Command Line Interface.

Data Extraction Engine

Data Extraction Engine is a LMS UTility that allows you to generate User Tracking data in XML format.

For more details, see Overview of Data Extraction Engine.

User Tracking Utility

Cisco Prime User Tracking Utility 2.0 is a Windows desktop utility that provides quick access to useful information about users or hosts discovered by LMS User Tracking application.

You can use UTU search band to search for the users or hosts in your network. You can search using user name, host name or IP address, or MAC address.

Various Acquisitions in User Tracking

This section explains the various acquisitions that can be done using LMS, to get information about the end users.

User Tracking Major Acquisition

Discovers all the end hosts that are connected to the devices managed by LMS.

For details on the various options that can be set before starting an acquisition, see Modifying UT Acquisition Settings.

User Tracking Acquisition can also be initiated from the CLI prompt. To do so, enter the following command:

NMSROOT/**campus/bin/ut -cli performMajorAcquisition -u** *userid* **-p** *password*

where *NMSROOT* is the directory where you have installed Cisco Prime. For more details, see User Tracking Command Line Interface.

User Tracking Minor Acquisition

Minor acquisition occurs on a device if any of the following changes take place:

- A new endhost or IP phone is added to the network.
- Port state changes (when the port comes up or goes down).
- A new VLAN is added to the network.
- There is a change in the existing VLAN.

Minor acquisition updates the LMS database with just the changes that have happened in the network. It is triggered at regular intervals. The default for these intervals is 60 minutes. You can configure the interval at which the acquisition takes place.

For details on modifying the acquisition interval, see Modifying UT Acquisition Schedule

User Tracking IP Phone Acquisition

Discovers all phones registered in Cisco Call Managers (CCM), that are managed by LMS.

Subnet based User Tracking Major Acquisition

User tracking subnet based acquisition would run only on those subnets that are configured in LMS. LMS discovers end hosts on all the VLANs available in the configured subnets.

Do subnet based acquisition, when you need details about the end hosts connected to a particular subnet or a select set of subnets. The acquisition completes faster, since it is not run on all devices managed by LMS.

For details on running subnet based acquisition, see Configuring UT Subnet Acquisition

Single device on-demand User Tracking Acquisition

This discovers the end hosts on all the VLANs available in the selected device. Hence this acquisition is useful for collecting information only on end hosts connected to the specified device.

For details on initiating this type of acquisition, see Configuring User Tracking Acquisition Actions

Using User Tracking Administration

You can perform the following administrative tasks using User Tracking Administration:

- Modify Acquisition settings.

  Before you start collecting information about the hosts in your network, you can set various options that control the way in which Acquisition happens.

  For example, you can set LMS to perform DNS lookup, while resolving the IP address of a host.

  For complete details, see Modifying UT Acquisition Settings

- Schedule Acquisition.

  You can set the day and time of the week when you want to run Major Acquisition. The time interval at which Minor Acquisition happens in the network can also be set.

  For more details, see Modifying UT Acquisition Schedule

- Configure Ping Sweep options for Acquisition.

  You can configure LMS to perform Ping Sweep on selected subnets, during Acquisition.

  For more details, see Modifying Ping Sweep Options

- Configure Subnet Acquisition.

  You can trigger acquisition on a single subnet or a select set of subnets. Subnet based acquisition collects details about the end hosts that are connected to a particular subnet or a select set of subnets. This Acquisition completes faster, since it is not run on all devices managed by LMS.

  For more details, see Configuring UT Subnet Acquisition

- Configure end host and IP phone data delete interval.

  You can modify the time interval for deleting entries from the End Host Table, IP Phone Table, or the History Table from the database.

  For more details, see Deleting User Tracking Purge Policy Details

- Configure UT Acquisition to discover end hosts connected to non-link trunk ports.

  Normally UT Acquisition only discovers end hosts that are connected to access ports. If you enable this feature, UT Acquisition also discovers end hosts that are connected to non-link trunk ports.

  For more details, see Configuring UT Acquisition in Trunk for End Host Discovery

- Specify Purge Policy.

  You can specify the intervals at which you want old reports and jobs to be purged. You can save the Purge Policy, so that the older jobs and archives are purged at the specified interval.

  For more details, see Specifying User Tracking Report Purge Policy

- Specify Domain Name display.

  You can specify the way in which domain names are to be displayed in User Tracking Reports.

  For more details, see Specifying Domain Name Display.

- Import information on end hosts.

  You can import user names and notes of end hosts that are already discovered by User Tracking, from a file.

  For more details, see Importing Information on End Host Users

- Enable Dynamic User Tracking.

  Dynamic Updates are asynchronous updates that are based on SNMP MAC notifications traps. LMS tracks changes about the end hosts and users on the network to provide real-time updates, based on these traps.

  For more details, see Understanding Dynamic Updates

- Enable Debugging options.

  When you face issues in running User Tracking, logging can be enabled for debugging purposes.

  For more details, see Debugging Options for User Tracking Server and Debugging Options for User Tracking Reports

Viewing User Tracking Acquisition Information

You can view acquisition information.

To view acquisition information:

Step 1 Either:

- Select **Admin > Collection Settings > User Tracking > Acquisitions Info**.

  Or

- Select **Inventory > User Tracking Settings > Acquisition Summary**.

The acquisition information appears with the following information:

Field	Description
Acquisition status	Status of the User Tracking Major Acquisition process. It can be either Idle or Running.
Last acquisition type	Type of User Tracking acquisition that you had performed last time. Types of acquisition are: • Major—User Tracking Major Acquisition • Devices—User Tracking Acquisition for a device • Subnets—User Tracking Acquisition for subnets • IP Phones—User Tracking Acquisition for IP phones
Acquisition start time	Date and time at which User Tracking started the Acquisition process. This is displayed in the format dd mon yyyy hh:mm:ss.
Acquisition end time	Date and time at which User Tracking stopped the Acquisition process. This is displayed in the format dd mon yyyy, hh:mm:ss time zone.
Number of acquisitions	Number of major and minor acquisitions performed.
Number of host entries	Number of hosts found after User Tracking acquisition.
Number of duplicate MAC	Number of MAC addresses that have duplicate entries in the list of hosts found.
Number of duplicate IP	Number of IP addresses that have duplicate entries in the list of end hosts found.
Number of CCM hosts	Number of Cisco CallManagers in the list of devices found after Data Collection.
Number of IP phone entries	Number of IP phones available in the LMS managed network.
Last Campus data collection completed at	Date and time of the previous LMS Data Collection process. This is displayed in the following format: dd mon yyyy hh:mm:ss time zone.
Data collection status	Status of the LMS Data Collection process. It can be either Idle or Running.

Configuring User Tracking Acquisition Actions

You can trigger the following acquisitions from this page:

- Device based Acquisition
- Subnet based Acquisition
- IP Phone Acquisition

To configure the required acquisition:

Step 1 Either:

- Select **Admin > Collection Settings > User Tracking > Acquisition Action**.

  Or

- Select **Inventory > User Tracking Settings > Acquisition Actions**.

The Acquisition Actions dialog box appears.

Step 2 Configure Acquisition Actions as specified in Table 7-1.

Table 7-1 Acquisition Actions

Field	Description	Usage Notes
Select a type	You can select the type of acquisition. Type of acquisition can be: • Device • Subnet • IP Phones	When you select a type of acquisition the appropriate fields are displayed.
Scope Selection	Select the All hosts and users check box to acquire information about all hosts and users in your network.	If you do not select the All hosts and users check box, the device selection field is enabled and you can enter the name or IP address of the device for which you require data.
Device Selection		
Device Name or IP Address	Enter the name or IP address of the device about which data is to be acquired.	Click **Select** to select the device from the list of available devices.
Subnets		
Type Selection	You can choose to get data about a particular subnet or about all the configured subnets.	If you choose to acquire data about a particular subnet, the subnet selection fields are enabled.
Subnet Selection		
Subnet ID	Select the IDs of the subnets on which you need to get data.	This field is enabled only if you select the Subnet option in the Type Selection area. Click **Select** to select the subnet ID from the list of available subnets.

Table 7-1 Acquisition Actions (continued)

Field	Description	Usage Notes
Subnet Mask	Enter the subnet mask.	If you select the subnet ID, the subnet mask is automatically entered.
Acquire Only VLAN Specific to Subnet	Select this check box to get data only about the VLANs specific to the subnet.	• If you select this check box, only the work stations associated with the VLANs that are mapped to the selected subnets will be acquired. • If you do not select this check box, work stations associated with all the available VLANs in the selected subnets will be acquired.

You do not have to specify any details for the IP Phones option.

Step 3 Click **Start Acquisition**.

Using User and Host Acquisition

You can modify the Acquisition settings and Acquisition schedule using the User and Host Acquisition option.

This section contains:

Modifying UT Acquisition Settings

You can modify User Tracking Acquisition settings.

This section contains:

Modifying Acquisition Settings from UI

To modify acquisition settings:

Step 1 Select **Admin > Collection Settings > User Tracking > Acquisition Settings**.

The Acquisition Settings dialog box appears.

Step 2 Modify the acquisition settings as specified in Table 7-2.

Table 7-2 Acquisition Settings Field Description

Field	Description	Usage Notes
Enable User Tracking for DHCP Environment	Enables User Tracking for DHCP Environment.	If you enable this property, it allows you to control inclusion and exclusion of Duplicate MAC addresses in the Acquisition. To understand the behavior of User Tracking in case of missing IP address, see UT Behaviour in DHCP Environment for Missing IP address. For details on properties that support Duplicate MAC addresses, see Configuring Properties That Support Duplicate MAC Addresses.
Enable User Tracking on Access Points	Enables User Tracking on Access Points	This is enabled by default and allows UT Major Acquisition process to collect Access point information. However, WlseUHIC cannot collect Wlse related end host information. If disabled, it precludes Access point acquisition. However, WlseUHIC collects Wlse related end host information.
Get user names from UNIX hosts	Select this option to allow Acquisition to collect the active usernames of UNIX hosts. UNIX user names are updated at the end of major acquisitions.	Collects information only for users, who are logged into the console port of the UNIX hosts.
Get user names from hosts in NT and NDS	Allows LMS to collect active user names on the Windows or Novell Directory Service (NDS) servers.	This option helps you to: • Collect information only for users who are currently logged into the network. • Collect information from NDS hosts. You must use NDS 5.0 or later. For this option you need to install the UTLite script.

Table 7-2 Acquisition Settings Field Description (continued)

Field	Description	Usage Notes
Use DNS to resolve host names	Resolves host names using DNS.	User Tracking performs DNS Lookup for a host to resolve its IP address. When you choose this option the Advanced button is enabled. Click on this to launch the Advanced UT Acquisition Settings window. The following options are available: • DNS threads Number of parallel threads allowed for name resolution. The default value is 1. Maximum number of threads allowed is 12. • DNS Timeout Time duration for which UT waits for a response from the DNS server, for name resolution. The value should be entered in milli seconds. The default value is 2000 milliseconds (2 seconds). Enter values and click **OK** to save changes.
User Port Number	Specify the UDP port number from where logon and logoff messages are received from hosts in Windows and NDS.	You must use the default port number unless it is already in use. This port number must match the port indicated in the login script.
Rogue MAC Detection	Enable notification when Rogue MACs are detected in the network.	LMS sends e-mails to the specified addresses, when unauthorized end hosts are detected in the network.
E-Mail	Specify the E-mail IDs to be notified when Rogue MACs are detected in the network.	You can enter multiple E-mail IDs separated by commas. This field is enabled only when you check the Rogue MAC Detection field.
Define Rogue MACs	Specify the list of Rogue MACs in the screen that is launched.	For details, see Configuring Rogue MAC List.
New MAC Detection	Enable notification when new MACs are detected in the network.	LMS sends e-mails to the specified addresses, when new end hosts are detected in the network.
E-Mail	Specify the E-mail IDs to be notified when new end hosts are detected in the network.	You can enter multiple E-mail IDs separated by commas. This field is enabled only when you check the New MAC Detection field.

Step 3 Click **Apply** to save the modifications in the settings.

Step 4 Click **Start Acquisition** to start User Tracking Acquisition with the modified settings.

UT Behaviour in DHCP Environment for Missing IP address

Selecting the **Enable User Tracking for DHCP Environment** *property* allows you to control inclusion and exclusion of Duplicate MAC addresses in UT Acquisition.

LMS will not get the IP address of end hosts, if the Router is not reachable or if it is excluded from DCR. In such cases, behaviour of User Tracking after enabling **Enable User Tracking for DHCP Environment** property, is explained in Table 7-3.

The conventions used in Table 7-3 are:

- MACx — MAC address of the endhost
- IPx — IP address of the endhost
- Device x — Device to which the end host is connected.
- Time in xx:xx format — Time entries in the Last seen column
- NA — Not Available.

Note The explanation given for scenarios 1 and 2 holds good, irrespective of the value set for *Enable User Tracking for DHCP Environment property.*

Table 7-3 UT Behaviour in DHCP Environment for Missing IP address

Scenario				Explanation	What gets Updated in Database			
Scenario1: Missing IP Address								
MAC1	NA	Device 1	6:35	For an endhost, if the IP address is not available in the first UT acquisition, but is available in the next, the IP address field in the database is updated with the value that is currently discovered.	MAC1	IP1	Device 1	6:40
MAC1	IP1	Device 1	6:40					
Scenario 2: Missing IP Address								
MAC1	IP1	Device 1	6:45	For an endhost, if the IP address is available in the first UT acquisition, but is not available in the next, the older value for IP address is retained in the database.	MAC1	IP1	Device 1	6:50
MAC1	NA	Device 1	6:50					
Scenario 3: Single MAC, Multiple IP Addresses								
MAC1	IP1	Device 1	6:55	For an endhost with Single MAC address but multiple IP addresses, if UT does not get the IP address in the current acquisition, it retains the older values in the database.	MAC1	IP1	Device 1	7:00
MAC1	IP2	Device 1	6:55		MAC1	IP2	Device 1	7:00
MAC1	IP3	Device 1	6:55		MAC1	IP3	Device 1	7:00
MAC1	NA	Device 1	7:00					
Scenario 4: Dynamic change in IP Address								

Table 7-3 UT Behaviour in DHCP Environment for Missing IP address

Scenario				Explanation	What gets Updated in Database			
MAC1	IP1	Device 1	4:00	For an endhost with different IP addresses at different points of time, if UT does not get the IP address in the current acquisition, it retains the value that was last discovered.	MAC1	IP1	Device 1	4:00
MAC1	IP2	Device 1	5:00		MAC1	IP2	Device 1	5:00
MAC1	IP3	Device 1	6:00		MAC1	IP3	Device 1	7:00
MAC1	NA	Device 1	7:00					
Scenario 5: Endhost moving between devices								
MAC1	IP1	Device 1	4:00	When an end host moves between devices, if UT does not find the IP address in the current acquisition, it retains the IP address value that was last discovered for that device.	MAC1	IP1	Device 1	6:00
MAC1	IP1	Device 2	5:00					
MAC 1	NA	Device 1	6:00					

Configuring Properties That Support Duplicate MAC Addresses

The following properties can be configured in the *ut.properties* file stored in

NMSROOT`/campus/etc/cwsi/`

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

Table 7-4 lists the properties that support Duplicate MAC Addresses

Table 7-4 Properties Supporting Duplicate MAC Addresses

Property	Description
UT.DuplicateMac.Include_SwitchPorts	List of switchports connected to endhosts, for which duplicate MAC entries need to be included in UT Major, UT Minor, UT device based, and UT subnet based Acquisition.
UT.DuplicateMac.Exclude_SwitchPorts	List of switchports connected to endhosts, for which duplicate MAC entries need to be excluded in UT Major, UT Minor, UT device based, and UT subnet based Acquisition.
UT.DuplicateMac.Include_Switches	List of switches connected to end hosts, for which duplicate MAC entries need to be included in UT Major, UT Minor, UT device based, and UT subnet based Acquisition.
UT.DuplicateMac.Exclude_Switches	List of switches connected to end hosts, for which duplicate MAC entries need to be excluded in UT Major, UT Minor, UT device based, and UT subnet based Acquisition.
UT.DuplicateMac.Include_Vlans	List of VLANs associated with endhosts, for which duplicate MAC entries need to be included in UT Major, UT Minor, UT device based, and UT subnet based Acquisition.

Table 7-4 Properties Supporting Duplicate MAC Addresses

Property	Description
UT.DuplicateMac.Exclude_Vlans	List of VLANs associated with endhosts, for which duplicate MAC entries need to be excluded in UT Major, UT Minor, UT device based, and UT subnet based Acquisition.
UT.DuplicateMac.Include_Subnets	List of subnets associated with endhosts, for which duplicate MAC entries need to be included in UT Major, UT Minor, UT device based, and UT subnet based Acquisition.
UT.DuplicateMac.Exclude_Subnets	List of subnets associated with endhosts, for which duplicate MAC entries need to be excluded in UT Major, UT Minor, UT device based, and UT subnet based Acquisition.

For the above list of properties:

- Values should be separated by commas.
- IP addresses of the devices should be given.
- Port numbers should be given along with the device IP address as *deviceip:port.*
- The Exclude list takes precedence over the Include list.

The usage scenario for the above lists is as follows:

- If you use the Include list OR the Exclude list alone, the duplicate MAC addresses will be included or excluded as specified.

  For example, if you set the Include list as,

  UT.DuplicateMac.Include_Switches=X,Y

  Duplicate MAC addresses will be allowed only for endhosts connected to Switches X and Y. Duplicate addresses will not be allowed for any other endhost.

- If you set both Include and Exclude list as,

  UT.DuplicateMac.Include_Switches=X,Y

  UT.DuplicateMac.Exclude_Switches=A,B

  Duplicate MAC addresses will not be allowed for endhosts connected only to Switches A and B. Duplicate addresses will be allowed for all other end hosts, even for those connected to switches not specified in the Include list. Thus when an Exclude list is set, the Include list is ignored.

The above examples hold good for the Include/Exclude lists of Switchports, Subnets and VLANs.

- The order of priority for the property list is as follows:
  a. SwitchPorts
  b. Switches
  c. VLANs
  d. Subnets

The SwitchPorts list has the highest priority, followed by Switches, VLANs and Subnets list.

For example, if you set

UT.DuplicateMac.Include_SwitchPorts=10.77.211.33:3/2

UT.DuplicateMac.Exclude_Switches=10.77.211.33

Although the switch 10.77.211.33 is in the Exclude list, a switchport belonging to that switch is also present in the Include list. So Duplicate MAC addresses will be allowed for that port on the switch. Thus the SwitchPorts list has higher priority over the Switches list.

Configuring User Tracking Properties from the Backend

This section explains the new user configurable properties that have been added to UT.

You can configure properties that control DNS name resolution and history reports, by editing them in the file *ut.properties*, stored in

NMSROOT`/campus/etc/cwsi/`

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

Table 7-5 lists the new properties added to UT:

Table 7-5 Configuring User Tracking Properties

Property	Default Value	Description
HistoryHostPurgeTime	10 days	Purges history entries that are older than the specified time. The value should be provided in minutes. For example, If you want to purge entries older than 10 days, set HistoryHostPurgeTime=14400
UT.nameResolution	both	Name resolution for end hosts using Java APIs JNDI and InetAddres.This property can have the following values: • wins (Use only InetAddress) • dns (Use only JNDI) • wins,dns (First InetAddress then JNDI) • both (JNDI first and InetAddress next)
UT.nameResolution.dnsTimeout	2000	Time duration for which UT waits for response from the DNS server, for name resolution. The value should be entered in milliseconds.
UT.nameResolution.winsTimeout	2000	Time duration for which UT waits for response from the DNS server, for name resolution.The value should be entered in milliseconds. This property must be enabled only for windows server.
UTMajorUseDNSCache	false	Uses cache memory for name resolution in subsequent User Tracking discoveries. User Tracking performs DNS Lookup for a host only if the IP address of the host is being resolved for the first time.It does not perform DNS Lookup for every Major Acquisition. This helps the application to reduce the number of queries during User Tracking Acquisition. This in turn reduces the time taken for Acquisition process.
UT.RunLookupAnalyzer	OFF	To analyze the performance of DNS servers and provide the following information in the *NMSROOT*\log\ut.log file: • 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 Set the value to ON to turn on the feature. You need not enable debugging for UT to get the LookupAnalyzer data in the ut.log file. For details on running Lookup Analyzer utility from the command prompt and example output of the utility, see Using Lookup Analyzer Utility

Configuring Rogue MAC List

MAC Addresses that are not authorized to exist in your network are termed as Rogue MAC addresses.

When you enable the Rogue MAC notification feature, you need to define the list of MAC addresses that are to be classified as unauthorized addresses in the network.

You can also import MAC addresses to Acceptable OUI either from a file or directly from UT.

If you import the MAC Addresses from a file or directly from UT, the MAC addresses in the file are converted to OUIs before you add them to the Acceptable OUI list.

To do so:

Step 1 Select **Admin > Collection Settings > User Tracking > Acquisition Settings**.

The User Tracking Acquisition settings window appears.

Step 2 Click **Define Rogue MACs.**

The Rogue MAC Configuration window appears. The lists displayed in the window are:

- Rogue MAC/OUI List
- Acceptable MAC/OUI List

Step 3 Click **Add MAC/OUI** to add new entries to the list.

The Add MAC/OUI window appears.

The Organizationally Unique Identifier (OUI) is a 24-bit number. It is used as an identifier to uniquely identify the vendor, manufacturer, or a worldwide organization.

An OUI reserves a block of each type of derivative identifier, such as MAC addresses, group addresses, and Subnetwork Access Protocol identifiers. It is used to identify a network interface controller (NIC), network protocol, or MAC addresses for Ethernet.

In case of MAC addresses, OUI is combined with a 24-bit number to form the address. The first three octets of the address are the OUI.

The Add MAC/OUI page is as explained in Table 7-6:

Table 7-6 Populating the MAC/OUI list

Property	Description
Select Mode	Provides the following options to add MAC addresses to MAC/OUI List: • Manual — Enables you to add MAC/OUI to either the Acceptable MAC/OUI List or to the Rogue MAC/OUI list. The Manual Add option is selected by default. • Import from file — Enables you to import MAC Addresses from a file to the Acceptable MAC/OUI List • Import from UT — Enables you to import MAC Addresses directly from UT to Acceptable MAC/OUI List
Add MAC/OUI	Enter the MAC Address or OUI in the text box provided. The values should be separated by spaces, tabs, or commas. You can also enter values on separate lines. The address can have only hexa decimal numbers separated by hyphen. Example: 00-c0-1d-99-06-b6
OUI List	Displays predefined values in LMS. You can select values from the list, to add to the Rogue OUI or Acceptable OUI list. To add more values to the list, add them to the Property file: *NMSROOT*/campus/etc/cwsi/OUI.properties where *NMSROOT* is the directory where you installed Cisco Prime. To get the latest OUIs listed by IEEE, see http://standards.ieee.org/regauth/oui/index.shtml

Step 4 Select any of the following:

- **Manual Add**

a. Select the required OUIs from the list displayed in OUI List.

b. Click either the **Add to Rogue MAC List** or the **Add to Acceptable MAC List**, based on your requirement.

The MAC or OUIs that you enter in the ADD MAC or in the OUI textbox will be added to the list that you selected.

- **Import From File**

a. Click **Browse** and browse to the folder location and choose the file to be imported

b. Click the Import to Acceptable OUI list.

The MACs are converted to OUIs before you add them to the Acceptable MAC/OUI list.

- Import From UT

Click the Import to Acceptable OUI list. The MACs are converted to OUIs prior to adding them to the Acceptable MAC/OUI List.

It is mandatory that the file that is imported to Acceptable MAC/OUI list must include the header - MAC Address followed by MAC Address entries.

For example: In the example, the file to be imported includes a MAC Address column with MAC Address entries.

MAC Address

MAC 1

MAC 2

MAC 3

The newly added values are reflected in the **Rogue MAC Configuration screen.**

Step 5 Check **Consider unqualified MAC as Rogue**

When you check this, LMS treats any new MAC address coming into the network as Rogue MAC. This is if it is not defined in the Acceptable MAC list.

Step 6 Click any of the following:

- **Save**

Saves the settings to the server. They come into effect in the next UT Major Acquisition cycle.

  - If Dynamic User Tracking is running, notification for new or Rogue MACs detected in the network, are sent immediately.
  - If WLSE is integrated with LMS, notification for wireless MACs detected in the network is sent.

- **Delete**

Deletes entries.

- **Cancel**

Cancels changes and closes the window.

Modifying UT Acquisition Schedule

You can modify UT acquisition schedule.

To modify acquisition schedule:

Step 1 Select **Admin > Collection Settings > User Tracking > Acquisition Schedule**.

The Acquisition Schedule dialog box appears.

Step 2 Start the user tracking major acquisition for all or failed devices as specified below:

- Select either **All devices** or **Failed devices** .
- Click **Start** to start the user tracking major acquisition immediately for the selected devices.

  The UT Acquisition Confirmation pop up appears.
- Click **OK** to start user tracking acquisition. A success message appears. Click **OK**.

  To cancel the user tracking acquisition process, click **Cancel**.

Step 3 Modify the acquisition schedule as specified in Table 7-7.

Table 7-7 Acquisition Schedule Field Description

Field	Description	Usage Notes
Minor Acquisition	Specify, in minutes, the periodicity at which a minor acquisition should take place.	None.
Major Acquisition	Specify the time at which a major acquisition is to take place. Specify the days of the week on which a major acquisition is to be scheduled.	None.
Days, Hour, Min	Days on which and the time at which a major acquisition is to be carried out.	You can add new schedules and edit or delete existing schedules.
Recurrence Pattern	Select the days of the week on which a major acquisition is to be scheduled.	This field is available only when you are adding or editing a schedule.

Step 4 Select the schedule and do any of the following:

- Click **Edit** to edit the schedule.
- Click **Delete** to delete the schedule.
- Click **Add** to add a new schedule.

Step 5 Click **OK** to save the changes or **Cancel** to cancel the changes.

Step 6 Click **Apply** after adding or editing a schedule.

Modifying Ping Sweep Options

A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to determine the range of IP addresses that map to live end hosts (computers). You can use a single ping to find out whether a specific end host exists on the network.

A Ping Sweep consists of ICMP (Internet Control Message Protocol) ECHO requests sent to multiple hosts. If a given address is live, it will return an ICMP ECHO reply. Ping sweeps are among the older and slower methods used to scan a network.

When Ping Sweep is enabled in LMS, the UTPing program in *NMSROOT*/campus/bin will be invoked during acquisition to send out a sweep of pings for each subnet.

Before collecting information from a device, the subnets connected to the device are pinged. This serves as a connectivity check, as well as loads the ARP table of the layer 3 device with the latest information. After pinging, acquisition process starts collecting end host information from the device.

To modify Ping Sweep options:

Step 1 Select **Admin > Collection Settings > User Tracking > Ping Sweep**.

The Ping Sweep dialog box appears.

Step 2 Choose any of the following:

- **Disable Ping Sweep**
- **Perform Ping Sweep on all subnets**
- **Exclude subnets from Ping Sweep**

  When you choose **Exclude subnets from Ping Sweep**, select the subnets that you want to exclude from Ping Sweep. You can select subnets from the list of available subnets and add to the list of subnets to be excluded.

Step 3 Specify the **Wait Interval**, if Ping Sweep is enabled.

Wait Interval is the time duration between pinging subnets. The interval ensures that the network is not flooded with ping packets.

For example, assume that you have included 4 subnets for pinging, and set the wait interval to 10 seconds.

If Subnets 1 and 2 are connected to Device 1, and Subnets 3 and 4 are connected to Device 2, then 10 seconds lapse between pinging Subnets 1 and 2. After pinging both the subnets, acquisition starts on Device 1. Same happens with Device 2.

Step 4 Click **Apply**.

User Tracking does not perform Ping Sweep on large subnets.

For more details, see Notes on Ping Sweep Option.

Notes on Ping Sweep Option

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.

Ping Sweep will not refresh the ARP cache, if firewall or Access Control List is enabled to block the ICMP packets to the network devices. Hence, User Tracking will not display the IP addresses of the associated hosts.

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.

You can increase the value of the wait interval. Wait interval helps the ping response traffic to settle, which may appear as Denial Of Service (DOS) or may affect the functioning of router by high CPU usage.

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, that will enable you to ping the host IP addresses. This will ensure that when you run User Tracking Acquisition the ARP cache of the router contains the IP addresses.

Configuring UT Subnet Acquisition

You can configure LMS to perform User Tracking Acquisition on selected subnets. These configurations are used for User Tracking Major Acquisition and *Configured Subnets* based acquisition. You can choose to include or exclude specified subnets to perform User Tracking major acquisition.

To configure Subnet acquisition:

Step 1 Select **Admin > Collection Settings > User Tracking > Subnet Acquisition Configuration**.

The Configure Subnet Acquisition dialog box appears.

Step 2 Select either of the following options:

- Perform acquisition on all subnets

  All the subnets are included for User Tracking Major Acquisition. If you select this option do not perform steps 4 and 5.

Or

- Perform Subnet-based acquisition

  The action depends on the Filter value.

Step 3 Select either of the following Filter values:

- Perform major acquisition on selected subnets

  All subnets added to the Selected Subnets list are included for User Tracking acquisition.

Or

- Do not perform major acquisition on selected subnets

  All subnets added to the **Selected Subnets** list are excluded for User Tracking acquisition.

Step 4 Select subnets from the list of **Available Subnets** and add them to the list of Selected Subnets.

In the User Tracking Acquisition Action page (**Admin > Collection Settings > User Tracking > Acquisition Action**), the Acquire Only VLAN Specific to Subnet check box is available.

- If you select this check box, only the work stations associated to the VLANs that are mapped to the selected subnets will be acquired.
- If you do not select this check box, work stations associated to all the available VLANs in the selected subnets will be acquired.

For more information, see Configuring User Tracking Acquisition Actions.

Step 5 Click **Apply**.

Deleting User Tracking Purge Policy Details

Using this option, you can modify the time interval and delete entries from the End Host Table, IP Phone Table, or the History Table from the database.

To delete user tracking purge policy details:

Step 1 Select **Admin > Network > Purge Settings > User Tracking Purge Policy**.

The Delete Interval dialog box appears.

Step 2 Specify delete intervals for end host, IP phone and history tables.

Step 3 Either:

- Click **Delete now** to delete the entries immediately.

  If you select this step do not perform Step 4.

Or

- Select **Delete After Every Major Acquisition**.

  If you select this option, LMS will delete records older than the specified interval, after every UT Major Acquisition.

Step 4 Click **Apply**.

Configuring UT Acquisition in Trunk for End Host Discovery

Normally UT Acquisition discovers end hosts connected only to access ports. If you enable this feature UT Acquisition discovers end hosts connected to non-link trunk ports also.

LMS classifies trunk ports as follows:

- Link ports — Trunk ports connected to Cisco devices (Switch or Router).
- Non-link ports— Trunk ports connected to end hosts or IP phones.

Scenarios where a Trunk port is connected to an end host:

In a switched network, many clients from different VLANs might access an enterprise resource, such as a database server.

If the server has only a standard EthernetNIC, it can belong to only one VLAN. Clients that belong to a different VLAN would have to send their traffic to a router. The router forwards the frames to the database server. The problem with this approach is the latency introduced by the router.

To overcome this, a trunk-capable NIC card can be placed in the server that understands multiple VLAN information. With this arrangement, an end station need not send its frame to the router. Instead it can directly access the file server. This makes the access much faster.

To configure trunk ports:

Step 1 Select **Admin > Collection Settings > User Tracking > Acquisition Configuration in Trunk**.

The Configure Trunk for End Hosts Discovery page appears.

Step 2 You can:

- Select **Enable End Host Discovery on all Trunks** to include all non-link trunk ports in UT Major Acquisition. After choosing this option, go to Step 8.
- Select **Enable End Host Discovery on selected Trunks** to include only the required set of non-link trunk ports in UT Major Acquisition. After choosing this option, go to Step 3.
- Select **Disable End Host Discovery on Trunks** to disable this feature. For this option, only the end hosts connected to access ports will be discovered by UT Major Acquisition. After choosing this option, go to Step 8.

Step 3 Select the list of switches where end hosts are connected to trunk ports, from the device selector.

Step 4 Click **Show Trunks**.

This displays the list of non-link trunk ports from the selected switches. Non-link trunk ports in down state are also listed here.

If you have selected devices that do not have non-link trunk ports, a message is displayed indicating the same. Change your selection to devices that have non-link trunk ports and click Show Trunks, to display the ports. Link ports are not listed here.

Step 5 Select the list of trunk ports where end hosts are connected from the Available Trunks list.

Step 6 Click **Add.**

The selected ports are displayed under the Selected Trunks list.

Step 7 Select either

- **Discover End Hosts on Trunks to include the selected ports in UT Major Acquisition.**

Or

- **Do not Discover End Hosts on Trunks** to exclude the selected ports from UT Major Acquisition.

Step 8 Click **Apply**.

This saves the configuration on the server.

After saving the configuration, run Data Collection. End hosts connected to trunk ports will be discovered in successive UT Major Acquisitions.

For Dynamic User Tracking to track end hosts connected to trunk ports, enable SNMP traps in these ports. For details on Enabling SNMP traps, see Enabling SNMP Traps on Switch Ports.

Importing Information on End Host Users

You can import from a file, user names and notes for end hosts already discovered.

To import information in end host users:

Step 1 Select **Admin > Collection Settings > User Tracking > Table Import**.

The End Host Table Import dialog box appears.

Step 2 Specify the name of the file from which you are importing the end host table data.

Step 3 Click **Apply**.

Note We recommend that you import a .CSV or .txt file. The imported file must have the following mandatory headers: MAC Address, User Name and Notes.
For example:
MAC1 Peter Finance department

Understanding Dynamic Updates

User Tracking generates reports on various functions and attributes of the end hosts and devices connected to your network that are managed by LMS. These reports are generated by polling the network at intervals set by the network administrator.

In addition to polling the network at regular intervals, LMS tracks changes in the end hosts and users on the network to provide real-time updates.

Dynamic Updates are asynchronous updates that are based on SNMP MAC notifications traps.

When an endhost is connected to a switch managed by LMS, an SNMP MAC notification trap is sent immediately from the switch to the LMS Server, indicating an ADD event. This trap contains the MAC address of the end host connected to the switch.

Similarly if an end host is disconnected from a switchport, an SNMP MAC notification trap is sent from the switch to the LMS indicating a DELETE event. Thus LMS provides real time data about end hosts coming into and moving out of the network.

Traps from suspended devices are not processed by LMS.

The difference between a UTMajor Acquisition and a Dynamic UT process is:

LMS collects data from the network at regular intervals for UTMajor Acquisition.

In Dynamic UT, the devices send traps to LMS as and when changes happen in the network.

This implies that you need not wait till next UTMajor Acquisition cycle to see the changes that have happened in your network. This is an improvement over the earlier versions, where updates on endhost information happened based on the polling cycle.

As a result of Dynamic updates, the following reports contain up-to-date information:

- End-Host Report

  Contains information from UT Major Acquisition and the recently added end-hosts.

- History Report

  Contains information from UT Major Acquisition and the recently disconnected end-hosts or end-hosts that have moved between ports or VLANs.

- Switch Port reports

  Contains information about the utilization of switch ports.

SNMP Traps are generated when a host is connected to the network, disconnected from the network or when it moves between VLANs or ports in the network.

To enable the Dynamic Updates feature:

- Switches must be managed by LMS.
- Configure LMS as a primary or secondary receiver of the MAC notifications. For details, see SNMP MAC Notification Listener.
- Configure all devices to send traps to the Trap Listener port of the LMS server (This is the port number that you would have configured on LMS Administration screen). For more details, see Enabling SNMP Traps on Switch Ports.
- Configure DHCP snooping on the switches

  Dynamic Host Configuration Protocol (DHCP) snooping is a security feature that filters untrusted DHCP message received from outside the network or Firewall, and builds and maintains a DHCP snooping binding table.

  LMS queries the CISCO-DHCP-SNOOPING-MIB to get the IP address of the end-host connected.

  For details on configuring DHCP, see

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_see/configuration/guide/scg.html

- User Tracking collects username and IP address through UTLite for Windows environment. For more details, see Understanding UTLite.

In a Windows environment you can either install UTLite or configure DHCP snooping to get IP address of the end host. They can also co-exist.

If you have neither installed UTLite nor enabled DHCP snooping, the IP address of the end-host connected will be updated only in the next UT Major Acquisition cycle. The ARP cache of the device should be populated with the IP address, for UT Major Acquisition to discover it.

The User Tracking Dynamic Updates process includes:

- MAC User-Host Information Collector (MACUHIC) Process
- User Tracking Manager (UTManager) Process
- UTLite

MAC User-Host Information Collector (MACUHIC) Process

MAC User-Host Information Collector tracks wired end users dynamically. It receives MAC notifications from the switches either directly or through LMS or HPOV.

After receiving the MAC notifications, MACUHIC validates the traps as follows:

- Checks whether the traps are generated from a switch managed by LMS.
- Checks whether the source is an access port.

If the traps are from valid sources:

- Updates LMS database.
- Informs UTManager if the trap is received for an ADD event.

User Tracking Manager (UTManager) Process

UTManager receives the information from MACUHIC about the ADD MAC notification trap that is received. This information is not complete and can be completed using updates from DHCP or UTLite or from both.

In the UTLite process, UTLite receives details of changes in username, and the time at which the host has logged in or logged out of the network.

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.

For complete information, see Understanding UTLite.

When an end-host is connected to your network, the following happens in the background.

1. The switch to which it is connected sends a MAC notification.
2. The MACUHIC process in LMS receives the MAC notification either directly from the switch or through other applications like LMS Monitor and Troubleshoot module or HPOV.
3. After processing this MAC notification, MACUHIC informs the UTManager.

4. LMS updates the database with the username and IP Address received from the UTLite. Database does not contain the complete information about the end host.
5. UTManager finds the following details:
   - Subnet, VTP domain, VLAN, Port duplex, and port speed from XML files generated after Data Collection.
   - Hostname from DNS Server

LMS updates the database with the complete User Tracking information for the host.

The User Tracking end host history reports, end host reports, reports on switch ports, wireless clients, duplicate MAC addresses, and duplicate IP addresses, use this updated information while generating reports.

Viewing Dynamic Updates Process Status

You can check whether the Dynamic Updates processes are running or not.

To check the status:

Step 1 Select **Admin > Collection Settings > User Tracking > Dynamic Update Process Status**.

The Dynamic Updates Process Status window appears.

If you have started the process already, the status window shows `Dynamic Updates Processes are RUNNING`.

Step 2 Click **Stop** to stop the Dynamic Updates processes.

The **Stop** button then toggles to **Start**, and the status window shows `Dynamic Updates Processes are STOPPED`. When you stop these processes, LMS stops processing traps sent by devices.

Step 3 Click **Start** to restart the Dynamic Updates processes.

The **Start** button again toggles to **Stop**.

Enabling SNMP Traps on Switch Ports

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, LMS processes only SNMPv1/SNMPv2 traps.

You can configure the ports CLI (see the Appendix Commands to Enable MAC Notification Traps on Devices) or Through LMS Interface.

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**.

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.

Note LMS supports only those switches that contain the Management Information Base (MIB) named MAC Notification, for enabling the SNMP traps.

Through LMS Interface

Prerequisites to enable MAC Notification on switches through LMS UI:

- The switches must be managed by LMS.

  If the devices are managed in SNMP version 2 (SNMPv2), you need to configure the Read as well as the Write community strings to enable MAC Notification in the switches.
- Configure the LMS server secondary credentials in LMS, you can set it up at **Admin > Collection Settings > Config > Secondary Credential Settings**. For more details, see Secondary Credentials.

Note LMS configures SNMP MAC Notification version 1 as the default version on switches for Dynamic Updates.

To enable MAC notification in switches:

Step 1 Select **Admin > Collection Settings > User Tracking > Device Trap Configuration**.

The Configure Trap on Devices dialog box appears.

Step 2 Select the switches for which you want to enable the traps, from the Device Selector.

Step 3 Click **Configure** to see the devices that you have selected.

Step 4 Click **Configure** to configure MAC notification on the ports in the devices.

The Configure MAC-Notification Trap on Ports dialog box appears. Table 7-8 describes the entries in the Configure MAC-Notification Trap on Ports dialog box.

Table 7-8 Configure MAC-Notification Trap on Ports Field Description

Field	Description
Add LMS Server as Trap Receiver	Check the check box to configure devices, to send SNMP traps to LMS. To configure LMS to listen to traps sent from devices, see Configuring SNMP Trap Listener.
Trap Community	Set a community string for the SNMP traps sent by devices. This property is enabled only when LMS is the Primary receiver for SNMP traps. This string is added to the list of valid strings in the Dynamic User Tracking Configuration screen.
Set as Dynamic User Tracking Default	Check the check box to make this community string as the default for future configurations, if LMS is the Primary Trap receiver.
Filter	Allows you to filter the ports listed, based on port name, device name and the device address (IP address of the device).
Trap Receiver Port	Port number that you entered for receiving traps. The default trap receiver port number of the LMS server is 1431.

Table 7-8 Configure MAC-Notification Trap on Ports Field Description (continued)

Field	Description
Port	Name of the port. Access ports as well as Non-link Trunk ports are listed.
Device Name	Name corresponding to IP address of the switch.
Device Address	IP address of the switch.
Rows per page	Select to view 10 to 50 rows on a page.

Step 5 Check the check boxes to select the ports that you want to enable SNMP traps.

Step 6 Click **Configure** to enable the SNMP traps.

An Information window appears.

Step 7 Click **OK**.

SNMP MAC Notification Listener

You must enable the switches to send SNMP MAC notifications to the listener, to avail the Dynamic Updates feature. After you enable the switches, you can choose either LMS Monitor and Troubleshoot module, or HP OpenView (HPOV) as the primary listener for MAC notifications.

- If you select LMS as the Primary listener, the MAC notifications reach the application directly from the switches.
- If you select LMS as the Secondary listener, (with HPOV or LMS Monitor and Troubleshoot module as the primary listener), MAC notifications reach LMS through HPOV or LMS Monitor and Troubleshoot module.

Note Even if the device is managed with SNMPv3, LMS processes only SNMPv1/SNMPv2 traps.

To select the MAC notification listener, see the following sections:

- Configuring SNMP Trap Listener
- HPOV as Primary Listener
- LMS Fault Monitor Module as Primary Listener

Configuring SNMP Trap Listener

LMS receives SNMP traps directly from the switches, unless you configure the port to direct the traps through HP Open View (HPOV) or Cisco Prime Monitoring Services.

To configure the trap listener:

Step 1 Select **Admin > Collection Settings > User Tracking > Trap Listener Configuration**.

The Trap Listener Configuration dialog box appears.

Step 2 Check **Listen traps from Device** to configure the trap reception directly from the devices

This makes LMS as the primary listener for receiving SNMP traps from devices.

OR

Check **Listen traps from Fault Monitor/HPOV** to receive the traps through these applications.

In this case, LMS Fault Monitor or HPOV act as the primary listener for SNMP traps from devices. They forward it to LMS which acts as the secondary listener for traps.

If both options are enabled, LMS can receive traps directly from devices, from HPOV and from LMS Fault Monitor module.

Step 3 Enter the port number of the port through which you want to receive the traps, in the Trap Listener Port field.

The default trap listener port number of the LMS server is 1431.

Step 4 Click **Apply** to save the details.

HPOV as Primary Listener

If you select HPOV as the primary listener, you must perform the following to receive the Dynamic Updates through LMS:

- Install Cisco Prime Integration Utility
- Install Trap Adapter for HPOV

The supported versions of HPOV are HPOV 7.50, HPOV 7.51 and HPOV 7.53.

Install Cisco Prime Integration Utility

You must have Cisco Prime Integration Utility (Integration Utility) installed on your system. Integration Utility is a utility that integrates Cisco Prime applications with third-party Network Management Systems (NMS).

This utility is available as part of the DVD in the LMS 4.1.

This integration utility adds Cisco device icons to topology maps, allows Cisco MIB browsing from NMS, and sets up menu items on the NMS to launch remotely installed Cisco Prime applications.

See *User Guide for CiscoWorks Integration Utility 1.7*, for more details on the integration utility.

Note You must install the Integration Utility on the same machine on which you have installed HPOV.

Install Trap Adapter for HPOV

LMS supports Trap Adapter for OpenView on Windows and Solaris operating systems.

To install the adapter on Windows:

Step 1 Locate the *TrapListener.conf* file in the *NMSROOT*`/campus/hpovadapter/WIN/` directory.

Step 2 Modify the Trap Receiver address and the port number to the LMS values, in the file.

Step 3 Set the *LIB* environment variable to *HP OpenView lib* directory.

Step 4 Run the **fwdTrap.exe** program located in the same directory.

The Trap Adapter gets attached to OpenView process and starts sending traps to the LMS server.

To install the adapter on Solaris/Soft Appliance:

Step 1 Locate *the TrapListener.conf* file in the /opt/CSCOpx/campus/hpovadapter/SOL directory.

Step 2 Modify the Trap Receiver address and the port number to the LMS values, in the file.

Step 3 Set the *LD_LIBRARY_PATH* environment variable to *HP OpenView lib* directory.

Step 4 Run the **fwdTrap** program located in the same directory.

The Trap Adapter gets attached to OpenView process and starts sending traps to the LMS server.

Supported Platforms (Operating Systems)

The supported platforms for the HP NNM and HPOV adapters are:

Network Management System	Supported Platforms
HP OpenView 9.1	• Solaris 10 • Windows 2008 R2 Standard x 64 Edition
HP OpenView 9.01	• Solaris 10 • Windows 2008 R2 Standard x 64 Edition
HP OpenView 9.0	• Solaris 10 • Windows Server 2008 x64 with Service Pack 2 • Windows Server 2008 x64 R2 with Service Pack 2

LMS Fault Monitor Module as Primary Listener

If you select Fault Monitor Module as the primary listener, you must perform the following to receive MAC Notifications.

The default port number of the Fault Monitor Module for receiving Traps from the switches is 9000. You must configure or verify this port number on the device, for the device to forward the Traps to the Fault Monitor Module. The trapd.conf file has the details of the port number that receives the Traps from the Fault Monitor server.

To enable Fault Monitor Module to forward the MAC Notifications, you must modify the trapd.conf file in the Fault Monitor Module server, at *NMSROOT*/object/smarts/conf/trapd directory. You can modify the file through the command line interface or through the application interface.

You can configure the application to forward the MAC Notifications to LMS Server in two ways:

- From LMS
- From the LMS Fault Monitor Server

From LMS

Step 1 Select **Admin > Network > Notification and Action Settings > Fault - SNMP trap forwarding**.

The Notification Services page appears.

Step 2 Enter the Hostname and the port number of the LMS server to which you want to forward the MAC Notifications.

Step 3 Click **Apply** to configure.

The trapd.conf file is modified and the DFMServer process is restarted.

Note If you configure through Cisco Prime, LMS server receives all Traps including MAC Notification.

From the LMS Fault Monitor Server

Step 1 Access the LMS Fault Monitor server using Telnet.

Step 2 Enter **`pdterm DfmServer`** at the command line to stop the LMS Fault Monitor server.

Step 3 Navigate to *NMSROOT*/object/smarts/conf/trapd directory.

Step 4 Edit the trapd.conf file in the directory to reflect the following changes.

Enter:

`FORWARD`: *address OID generic type specific type* \ *host* [:*port*] | [:*port*:*community*] [*host* [:*port*] | [:*port*:*community*] ...], where the explanation for each variable is provided in the trapd.conf file.

Step 5 Enter **`pdexec DfmServer`** at the command line to restart the LMS Fault Monitor server.

Configuring Dynamic User Tracking

You can configure certain properties in Dynamic User Tracking to enhance the security of the system. These properties make the server receive traps only from specified devices and with specified community strings.

To configure properties for filtering SNMP Traps:

Step 1 Select **Admin > Collection Settings > User Tracking > Dynamic User Tracking Configuration**.

The Dynamic User Tracking Configuration page appears.

Step 2 Select the **Validate SNMP Community** check box**.**

LMS validates the community string in SNMP traps, with the values you have set**.** You can add community strings only after checking this check box.

- If you configure a device with SNMP v2 or v1 settings in DCR, then the device is initially queried with SNMP v2 by LMS. If the query fails, LMS will query the device with SNMP v1.
- If you configure a device with SNMPv3 settings in DCR, then the device is queried with SNMP v3. However, if the query fails, the same device will not be queried with SNMP v2 or v1.

Step 3 Enter the community string in the **Valid Community List** text box and click **Add**.

You can add the community strings one at a time. You can use the **Delete** button to remove the extra or erroneous strings.

The default Trap community string that you might have added in the Device Trap configuration screen is also listed here.

Step 4 Select the **Validate Trap Source** check box**.**

LMS validates the source IP Address of the trap. You can add the list of IP Addresses only after checking this check box.

Step 5 Enter the IP Address in the text box provided and click **Add**.

You can use the Delete button to delete extra or erroneous entries.

Step 6 Click **Apply to save changes to the server.**

To revert to the default values, click **Reset**.

You can use any one of the options to filter SNMP traps.

For example:

To process traps from all sources, and that have private or test as the community string, set

```
Validate SNMP Community = true (by checking the check-box)
Community String = private, test
Validate Trap Source =false
```

then traps from all sources with community string private or test will be processed by LMS.

To process traps from the listed IP addresses, with the community string private or test set:

```
Validate SNMP Community =true
Community String = private, test
Validate Trap Source =true
Valid IP Addresses = 10.77.210.211, 10.77.210.212
```

then *traps from the listed IP addresses, with the community string private or test will be processed by LMS. In this case, LMS first validates the community string, and if it matches, validates the source address.*

Using User Tracking Utility

Cisco Prime User Tracking Utility (UTU) is a Windows desktop utility that provides quick access to useful information about users, hosts, or IP Phones discovered by LMS User Tracking application.

This section contains the following:

Understanding UTU

User Tracking Utility (UTU) allows users with Help Desk access to search for users, hosts, or IP Phones discovered by LMS User Tracking application. UTU comprises a server-side component and a client utility.

UTU is supported on LMS 3.0 (Campus Manager 5.0.6), LMS 3.1 (Campus Manager 5.1.4), and LMS 3.2 (Campus Manager 5.2.1). To use UTU in LMS 4.1, Network Topology, Layer 2 Services and User Tracking must be enabled and accessible through the network.

UTU 2.0 supports silent installation mode for easy deployment. It supports communication with LMS server in Secure Sockets Layer (SSL) mode.

The following are the list of features supported in the Cisco Prime User Tracking Utility 2.0 release:

Windows Vista Support

Earlier, User Tracking Utility did not work on Windows Vista client systems because of library conflicts.

UTU 2.0 is built on Microsoft .Net Framework and Windows Presentation Foundation (WPF). With this, UTU 2.0 now works on Windows Vista client systems

Support for Phone Number Search

In this release, UTU supports searching phone numbers in addition to existing search criteria.

Hardware and Software Requirements for UTU

Table 7-9 lists the minimum system requirements for UTU.

Table 7-9 System Requirements for UTU

Requirement Type	Minimum Requirements
System hardware	IBM PC-compatible computer with Intel Pentium processor.
System software	• Windows 2008 • Windows XP with SP2 or SP3 • Windows Vista
Memory (RAM)	512 MB
Additional required software	• LMS 3.0 (Campus Manager 5.0.6), or LMS 3.1 (Campus Manager 5.1.4), or LMS 3.2 (Campus Manager 5.2.1), or LMS 4.1 (Network Topology, Layer 2 Services and User Tracking) • Microsoft .Net Runtime 3.5 Service Pack 1 You can download Microsoft .Net Runtime 3.5 Service Pack 1 from http://www.microsoft.com
Network Connectivity	LMS 3.0 (Campus Manager 5.0.6) or LMS 3.1 (Campus Manager 5.1.4) or LMS 3.2 (Campus Manager 5.2.1) or LMS 4.1 (Network Topology, Layer 2 Services and User Tracking) must be running, and accessible through the network

Downloading UTU

UTU requires Cisco PrimeUserTrackingUtility2.0.exe file to be downloaded and installed.

To download UTU 2.0:

Step 1 Click http://www.cisco.com/cisco/software/navigator.html.

You must be a registered Cisco.com user to access this Software Download site. The site prompts you to enter your Cisco.com username and password in the login screen, if you have not logged in already.

Step 2 Select the Software Product Category as Network Management and Automation.

Step 3 Select **Routing and Switching Management > Network Management Solutions > Cisco Prime LAN Management Solution 4.0 and later** from the product tree.

Step 4 Select Cisco Prime LAN Management Solution 4.1.

Step 5 Select the appropriate product software type.

Step 6 Select a product release version from the Latest Releases folder and locate the software update to download.

Step 7 Locate the file CiscoWorksUserTrackingUtility2.0.zip

This zip file contains CiscoWorksUserTrackingUtility2.0.exe and setup.iss file (required for silent installation).

Step 8 Click the Download Now button to download and save the device package file to any local directory on LMS Server.

Step 9 Extract the file using any file extractor such as WinZip.

Installing UTU

You can install UTU 2.0 either in normal installation mode or silent installation mode.

Before you install UTU 2.0, check whether you system meets the requirements mentioned in Hardware and Software Requirements for UTU.

This section explains:

- Installing UTU in Silent Mode
- Installing UTU in Normal Mode

Installing UTU in Silent Mode

To install UTU in silent mode, run the following command at the command prompt:

exe-location`\CiscoWorksUserTrackingUtility2.0.exe -a -s -f1`*file-location*`\setup.iss`

where

- *exe-location* is the directory where you have extracted the CiscoWorksUserTrackingUtility2.0.exe file
- *file-location* is the directory where you have the setup.iss file.

Do not use space after the `-f1` option. Use the complete path for *file-location*.

For example, if the install directory for UTU is c:\utu, enter the following at the command prompt:

```
c:\utu\CiscoWorksUserTrackingUtility2.0.exe -a -s -f1c:\utu\setup.iss
```

Editing Setup.iss File

UTU is installed in the C:\Program Files\CSCOutu2.0 directory, by default.

If you want to install UTU in some other directory, you must edit the content of the setup.iss file. Change the value of the szDir attribute in the setup.iss file.

For example, if you want to set the installation directory as D:\utu20, change `szDir=C:\Program Files\CSCOutu2.0` to `szDir=D:\utu20` in the setup.iss file.

Setup.log File

The setup.log file is created during the installation in the same directory where you have extracted the setup.iss file.

You should see the setup.log file to check the installation completion status.

The value of the ResultCode attribute in the setup.log informs you whether the installation has completed successfully. The value 0 denotes that the UTU installation in silent mode is successful.

When the value of the ResultCode attribute is other than 0, you must install UTU again.

Installing UTU in Normal Mode

To install UTU in normal installation mode:

Step 1 Log into the system with local system administrator privileges.

Step 2 Navigate to the directory that contains CiscoWorksUserTrackingUtility2.0.exe.

Step 3 Double-click CiscoWorksUserTrackingUtility2.0.exe to begin installation.

The User Tracking Utility Welcome screen appears.

Step 4 Click **Next**.

A warning message appears if you have not installed .Net Framework 3.5 SP1.

You can install .Net Framework 3.5 SP1 after terminating the current UTU installation or before completing the current UTU installation.

Step 5 Click **Next**.

A confirmation message appears.

Step 6 Click **Yes**.

The Choose Destination Location dialog box appears. By default, UTU is installed in the directory C:\Program Files\CSCOutu2.0.

Note If you have installed .Net Framework 3.5 SP1 already on the system, the installer directs you to the Choose Destination dialog box, when you click Next in the User Tracking Utility Welcome screen.

If you click No in the confirmation message, the warning message appears again stating that you have not installed .Net Framework 3.5 SP1.

You can download and install .Net Framework 3.5 SP1. and then continue with the UTU installation.

Step 7 Click **Next** to install UTU in the default directory.

or

a. Click **Browse** to choose a different directory and click **OK.**

b. Click **Next** to continue with the installation.

The installation continues.

Step 8 Click **Finish** to complete the installation. User Tracking Utility is installed at the destination location you specified in Step 7 above and a shortcut to UTU is created on the desktop. To access the utility, see Accessing UTU.

Accessing UTU

To access UTU, click either:

- **Start > Programs > Cisco Prime UTU 2.0 > Cisco Prime User Tracking Utility 2.0**

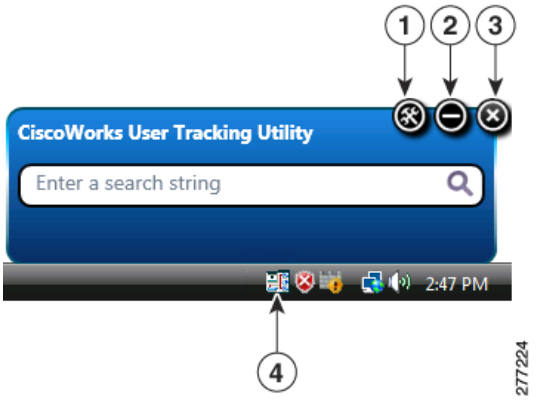
Or

- UTU 2.0 shortcut available on the desktop

The UTU band appears. See Figure 7-1 for UTU 2.0 band.

You can also find an icon in the task bar. You can use this icon to restore the UTU band when minimized.

Figure 7-1 User Tracking Utility - Search Band



1 - Settings Icon
2 - Minimize icon
3 - Close icon
4 - UTU task bar icon

After a system restart and during the startup, the system launches the UTU automatically.

Configuring UTU

You must configure UTU to set the Campus Manager (for releases earlier than LMS 4.0), or LMS 4.1 server configurations.

To configure UTU:

Step 1 Click the Settings icon.

Or

a. Right-click the UTU search band.

A popup menu appears.

b. Click **Settings**.

The Cisco Prime Server Settings dialog box appears.

Step 2 Enter the name or IP Address of the server on which Campus Manager (for releases earlier than LMS 4.0), or LMS 4.1 is installed.

Step 3 Enter the port number of the LMS Server.

The default HTTP port number is 1741.

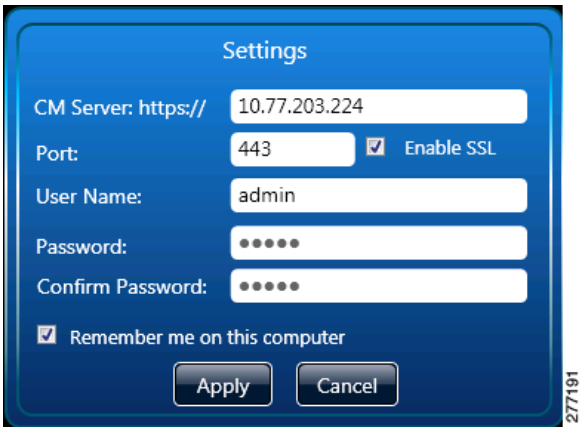
You can modify the port number if required.

Step 4 Click **Enable SSL** for communicating with an SSL enabled server.

The port is changed to 443, which is the default port for SSL.

You can modify the port number if required. See Figure 7-2.

Figure 7-2 Enabling SSL



Step 5 Enter a valid Cisco Prime Server user name and password.

This is used to verify the validity of the user when searching for users, hosts, or IP Phones.

Step 6 Confirm the password by re-entering it.

Step 7 Select the Remember me on this computer checkbox if you want the client system to remember your credentials.

The credentials are preserved only for the current user of Windows system. The credentials are not available when you log into the Windows system with a different user name.

Step 8 Click **Apply** to save the changes.

Searching for Users, Hosts or IP Phones Using UTU

You can use the UTU Search Band to search for the users, hosts, or IP Phones in your network.

Note UTU search is case-insensitive.

To search for users, hosts, or IP Phones:

Step 1 Right-click the UTU search band.

A popup menu appears with the default search criterion **Host name/IP Address** selected.

Step 2 Select a search criterion from the popup menu.

You can search using:

- User name
- Host name or IP Address
- Device name or IP Address
- MAC Address
- Phone number

The default search criterion is host name or IP Address of the host.

The selected criterion is set for future searches until you change the criterion.

Step 3 Enter any value related to user name, host name, device name, IP Address, Phone number or the MAC Address in the UTU search field.

For example, you can enter **10.77.208** in the search field.

Step 4 Press **Enter**.

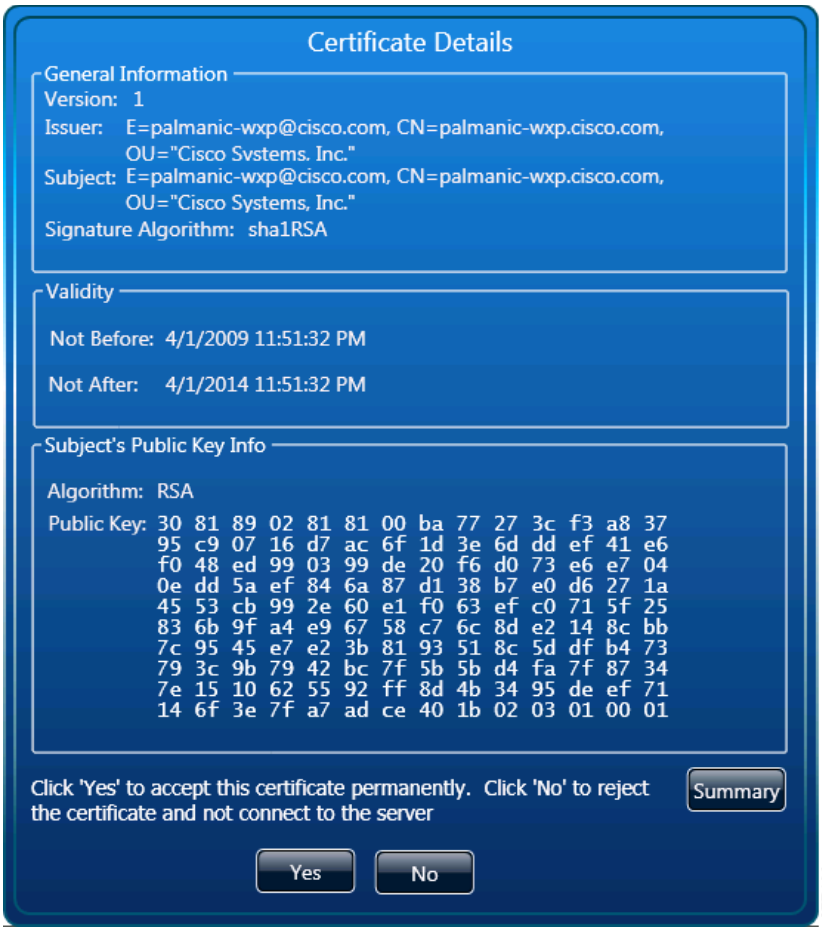
If your server is not SSL enabled, go to Step 7.

When you query for data from an SSL enabled server, the Certificate Summary dialog box appears.

Step 5 Click **Details** to view the certificate details.

You can verify the authenticity and correctness of the SSL server here. See Figure 7-3.

Figure 7-3 Certificate Details



You can click **Summary** to go back to the Certificate Viewer dialog box.

Step 6 Click **Yes** in the Certificate Viewer dialog box or Certificate Details dialog box to accept and store the certificate.

SSL connection is established with the server.

If you click **No**, the certificate is not stored and no connection is established with the server.

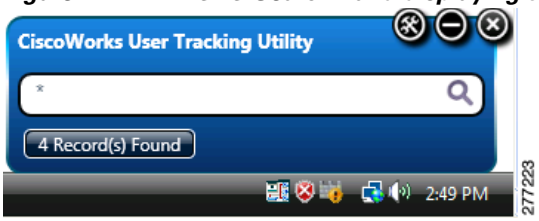
Note The Certificate Viewer dialog box appears only for the first time configuration. If you had clicked **Yes** the first time, you are not prompted to store the certificate during subsequent sessions.

Step 7 Click the *X* Record(s) Found button to launch the results window.

X denotes the number of matches found.

For example, if there 4 matches found, the UTU Search band displays 4 Record(s) Found. See Figure 7-4.

Figure 7-4 UTU Search Band displaying the number of matching records



UTU search returns only the top 500 records if the number of matches exceed 500. You must refine your search if you want better and more accurate results.

Step 8 Select an entry in the Results window.

UTU displays the search results, which is a list of user names, host names, IP Addresses, or MAC Addresses, in a Results window.

The Results window has the following options:

- **Copy to Clipboard**, where you can copy the selected search result record.
- **Copy All to Clipboard**, where you can copy all the search result records.
- **Close**, which you can use to close the window.

For a selected search result record, the Results window displays the details as described in:

- Table 7-10 for all search criteria except Phone Number
- Table 7-11 for search based on Phone Number

See Figure 7-5 for MAC Address search results window and Figure 7-6 for IP Phone search results window.

Table 7-10 Details for Each Entry in Results Window For a User or Host Search

Entry	Description
User Name	Name of the user logged in to the host.
MAC Address	Media Access Control (MAC) address of network interface card in end-user node.
Host IP Address	IP Address of the host.
Host Name	Name of the host discovered by User Tracking.
Subnet	Subnet to which the host belongs.
Subnet Mask	Subnet mask of the host
Device name	Name of the switch.
Device IP Address	IP Address of the switch
VLAN	VLAN to which the port of the switch belongs.
Port	Port number to which the host is connected.
Port Description	Description of the port number to which the host is connected.
Port State	State of the port: Static or Dynamic.
Port Speed	Bandwidth of the port of the switch.

Table 7-10 Details for Each Entry in Results Window For a User or Host Search

Entry	Description
Port Duplex	Port Duplex configuration details on the device.
Last Seen	Date and time when User Tracking last found an entry for this user or host in a switch. Last Seen is displayed in the format yyyy/mm/dd hh:mm:ss.

Figure 7-5 MAC Address Search Results Window

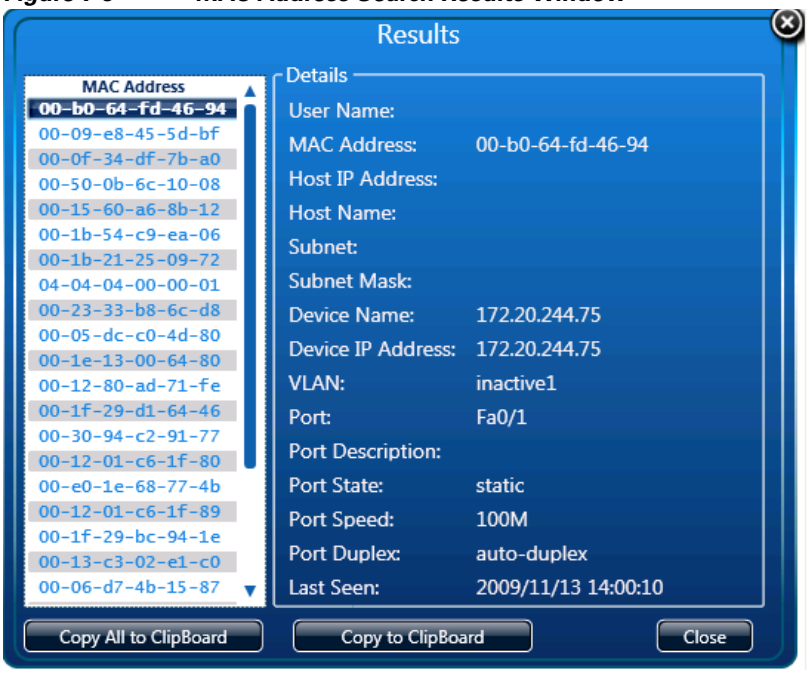


Table 7-11 Details for Each Entry in Results Window For a Phone Number Search

Entry	Description
Phone Number	IP Phone number
MAC Address	Media Access Control (MAC) address of network interface card on the phone.
Phone IP Address	IP Address of the phone.
CCM Address	IP Address of the Cisco Call Manager
Status	Status of the phone, as known to Cisco Call Manager
Phone Type	Model of the phone. Can be SP30, SP30+, 12S, 12SP, 12SPplus, 30SPplus, 30VIP, SoftPhone, or unknown.
Phone Description	Description of the phone.
Device Name	Name corresponding to IP Address of device.
Device IP Address	IP Address of the device
Port	Port number to which the phone is connected.

Table 7-11 Details for Each Entry in Results Window For a Phone Number Search

Entry	Description
Port Description	Description of the port to which the phone is connected.
Last Seen	Date and time when User Tracking last found an entry. Last Seen is displayed in the format yyyy/mm/dd hh:mm:ss.

Figure 7-6 IP Phone Number Search Results Window

Note The search results for the value you enter in the search field depends on the default search criteria.

Using Search Patterns for UTU

UTU searches for the users, hosts, or IP Phones that match the search criterion. See Searching for Users, Hosts or IP Phones Using UTU for more information.

You can search for users, hosts, or IP Phones by entering a search pattern or substring of a search pattern.

For example, entering **Cisco** displays host names that start with, end with or contain Cisco for a search on host names.

You do not have to use wildcard character * to match a pattern or substring of the pattern.

To search for a MAC Address, you can use one of the following MAC Address patterns or a substring of these patterns:

- *xxxx.xxxx.xxxx*
- *xx:xx:xx:xx:xx:xx*
- *xxxxxxxxxxxx*
- *xx-xx-xx-xx-xx-xx*

Here *x* denotes a hexadecimal number.

Uninstalling UTU

Ensure that UTU is not running while uninstalling.

If you try to uninstall UTU when it is running, an error message appears and uninstallation terminates.

To uninstall UTU:

Step 1 Select **Start > Programs > Cisco Prime UTU 2.0 > Uninstall Cisco Prime User Tracking Utility 2.0** from the windows task bar.

The Uninstallation wizard appears and prompts you to confirm the UTU uninstallation.

Step 2 Click **Yes**.

The Uninstallation continues.

Step 3 Click **Finish** to exit the uninstallation wizard.

Upgrading to UTU 2.0

You can install UTU 2.0 on the same system where UTU 1.1.1 is installed.

You can choose to install UTU 2.0 on any directory other than the directory where UTU 1.1.1 is installed.

See Installing UTU for installation instructions.

Re-installing UTU 2.0

Re-installation of UTU 2.0 is supported on the normal mode of installation.

In the normal mode of installation, you are prompted with a confirmation message to continue the installation. You must provide your inputs to continue the installation.

See Installing UTU for installation instructions.

The user profiles that are created are not lost during re-installation.