CHAPTER 5

User and Device Network Access Reporting

Understanding who is accessing the corporate network, what they are using, and where they are connected allows customers to better understand:

- Current port utilization of the network
- Movement of employees and devices on the network
- Suspicious or unauthorized access of the network
- Location of missing or even stolen assets, such as on a college campus
- Location of unknown devices on the network

Adding historical logging of when users and devices are accessing the network allows:

- Historical port utilization data
- Persistent records of when users and devices accessed specific locations in the network
- Searchable data of historical access for troubleshooting and asset tracking

CiscoWorks LAN Management Solution 4.0 provides a single point for user and device monitoring and tracking data to be collected, organized, and displayed.

CiscoWorks Lan Management Solution 4.0

CiscoWorks LAN Management Solution 4.0 (LMS) is an integrated suite of management functions that simplifies the configuration, administration, monitoring, and troubleshooting of an end-to-end borderless network. The solution aligns management functionality with the way network operators do their jobs.

This document focuses on the user tracking features of LMS to monitor and log who is accessing the network, from where, with what, and when.

LMS User Tracking

User Tracking tracks wired end hosts, which might include PC workstations, IP phones, medianet endpoints, and other devices as well as Windows-based users on the network.

Table 5-1 illustrates what can be expected from the user tracking features of LMS:

Table 5-1 User Tracking Features

Who	Username of Windows-based clients
What	Device MAC, IP, and hostname
Where	Switch and port to which device is connected
When	Historical access logs showing when and where devices and users are connecting and disconnecting

User Tracking—End Device Tracking and End User Tracking

While the overall feature is called User Tracking, it can really be described as a combination of End Device Tracking and End User Tracking, which are the terms used in this document for clarity. Within the LMS product and documentation, the term User Tracking is used to refer to all of the features and capabilities discussed in this document.

- End Device Tracking is of the actual end device hardware connecting to the wired network.
- End User Tracking adds the user name of users logging in and out through Windows-based end devices.

End Device Tracking may be implemented without End User Tracking, but not vice versa. End User Tracking relies on and compliments End Device Tracking information in the LMS database.

Table 5-2 shows the primary information provided by End Device Tracking and End User Tracking.

Table 5-2 Information Provided by Tracking Types

User Tracking	
End Device Tracking	**End User Tracking**
MAC address/IP address/hostname	MAC address/IP address/hostname
Switch/port/VLAN	Username

The first rows are identical, providing the MAC address, IP address, and hostname. The primary reason for the duplication is to match the user to the device in LMS. The secondary reason is to fill in any missing information.

For example, End Device Tracking relies on reverse DNS to populate the device hostname. The End User Tracking information is matched to an end device in the LMS database via the MAC address. If the device is not listed in DNS, such as a DHCP-enabled client workstation, End User Tracking will populate the hostname in LMS. If the IP address has not been acquired from ARP cache by End Device Tracking, End User Tracking will populate that as well.

User Tracking Functionality Detail

End Device Tracking

End Device Tracking represents the majority of the User Tracking functionality in LMS. Three main processes are used to gather and maintain end device information:

- Major acquisitions—Scanning all ports on all devices
- Minor acquisitions—Scanning for changes
- Dynamic updates—SNMP traps sent to LMS from access devices as end devices connect and disconnect

End Device Scheduled Updates

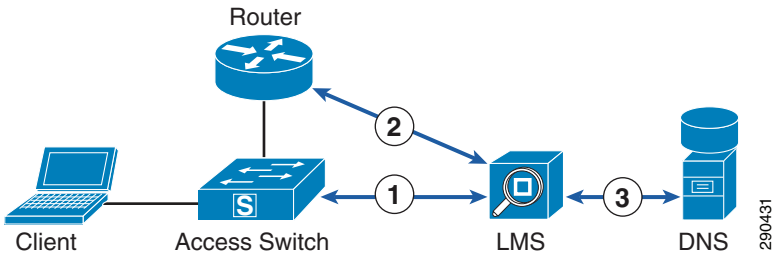
Scheduled updates include major acquisitions and minor acquisitions. For both of these operations, LMS accesses all devices it manages by default. Devices may be explicitly defined in LMS or discovered through a robust discovery mechanism. For more information about device management, see Product Documentation.

Major acquisitions are executed based on a user-defined schedule, which could be anywhere from once per week to every few hours. Major acquisitions look at every port on every access device known to LMS. If all access devices are managed by LMS and set to send dynamic updates to LMS, the interval for major acquisitions may be set to once per day or longer.

Minor acquisitions are executed based on a smaller time interval, defaulting to once per hour. Minor acquisitions only look at changes on the access devices.

Figure 5-1 illustrates the flow of events during scheduled updates.

Figure 5-1 Event Flow During Scheduled Updates



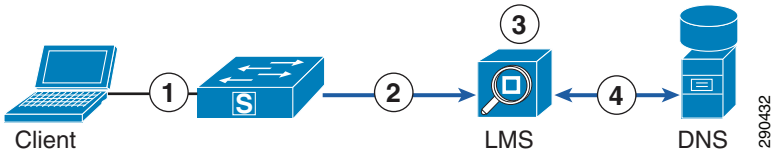
1. LMS executes a query of access devices to pull back MAC addresses associated with ports.
2. LMS executes a query of Layer 3 devices to pull back ARP tables.
3. LMS uses this information to correlate MAC addresses to IP addresses and performs reverse DNS lookups to obtain hostnames.
4. LMS populates the database with obtained data for User Tracking reporting.

End Device Dynamic Updates

Dynamic updates are the most important, providing current and accurate information as to what devices are connected and where. These updates are initiated from the access devices via SNMP traps sent to a special listener on LMS. When an end device connects or disconnects from an access device, that access device immediately sends a trap to LMS. LMS then immediately updates the device tracking information in the database, recording the event for both historical tracking as well as reports reflecting current devices connected. The update is visible in current device tracking reports within 30 seconds of the event.

Figure 5-2 illustrates the flow of events during dynamic updates.

Figure 5-2 Event Flow During Dynamic Updates



1. Access device generates a SNMP trap when a client device is connected to a port, sending the device MAC address with port information to LMS.
2. LMS receives this trap and enters it into the database.
3. LMS matches the MAC address to an IP address if an entry exists in the previously-obtained ARP tables.
4. If an IP address exists, LMS performs a reverse DNS lookup to obtain the hostname.
5. LMS populates the database with the obtained data for User Tracking reporting.

End User Tracking

End User Tracking uses a Windows process on the client to track actual users as they log in and out from Windows-based end devices, matching their information to the end device they are using. This is accomplished by a process initiated on the end host when the user logs in and a login script executes.

The process, called UTLite, sends an initial update to LMS upon user login, followed by continuous updates every 10 minutes to maintain the active login state for that user in LMS. Upon logout, the UTLite process sends an update indicating the logout process occurred, removing the active state in LMS, and moving that login event to the archives for historical tracking purposes.

If the host is disconnected from the network without the user logging out, LMS will stop receiving updates from the UTLite process and will determine that the user is no longer active on the network.

End User Tracking is always dynamic since the end host sends the end user information to LMS unsolicited.

End User Tracking and End Device Dynamic Updates

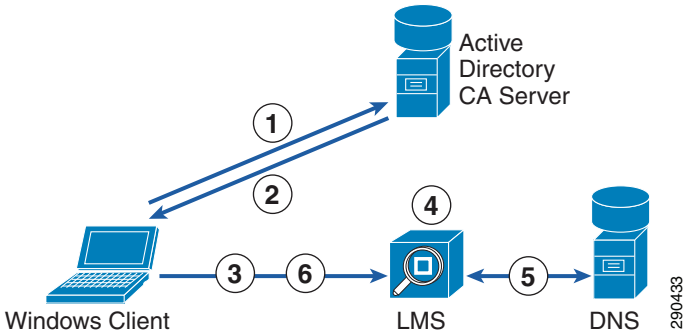
End Device Dynamic Updates, discussed earlier, must be implemented for End User Tracking to function correctly. The information delivered to LMS by End User Tracking is matched to an existing end device in the database. If the end device does not exist, the user tracking data is not recorded.

Without End Device Dynamic Updates implemented, devices connecting to the network will not be recorded until a Scheduled Minor Update runs. If the end device is disconnected before the scheduled update runs, the record of that user connecting to the network will be lost. Implementing End Device Dynamic Updates prevents this by inserting the device into the LMS database before the UTLite process sends the End User Tracking information to LMS.

End User Tracking UTLite Process

Figure 5-3 illustrates the flow of events during logging of individual user access with the UTlite process.

Figure 5-3 Flow of Events During Logging of Individual User Access

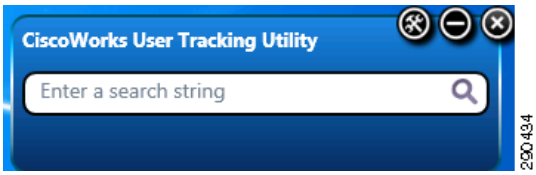


1. Client logs into a domain.
2. Domain script runs, executing the UTlite process on the client.
3. The UTlite process running on the client sends UDP packets to the LMS server with the following client information:
   - User ID
   - Domain
   - MAC address
   - IP address
4. LMS then uses this information to correlate the user information to a device in its database by matching the MAC address and then consolidates the information, filling in User ID, Domain, and IP address.
5. LMS will then do a reverse DNS lookup to fill in the hostname, if it exists in DNS.
6. Upon logout, the UTlite process running on the client notifies LMS, terminates LMS functionality to record when the client logged out of the domain, and removes the username from the active device entry in the database.

User Tracking Utility (End Device and End User)

The User Tracking Utility is a Windows-based utility used to search the User Tracking data in LMS. The User Tracking Utility lets an administrator using a Windows client workstation enter search criteria to locate end devices. The main interface of the User Tracking Utility is a simple search box as shown in Figure 5-4.

Figure 5-4 User Tracking Utility Main Interface



After searching for a client, the results are displayed as illustrated in Figure 5-5.

Figure 5-5 Results Screen

The User Tracking Utility is a simple search utility, not a real-time tracking utility. Device and user information is shown only as a result of a search using some criteria already known to the administrator, such as client hostname.

User Tracking Reporting (End Device and End User)

User Tracking Reporting allows you to see all hosts, some hosts, or a single host based on how you generate the report. Reports may be generated showing active end devices and users currently connected to the network as well as past connections, which is discussed in the next section.

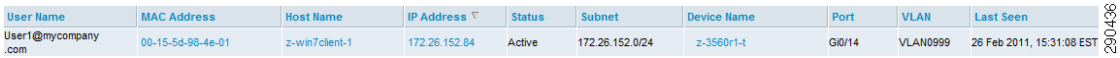
Reports for active users and devices may be customized to include or exclude specific information about the clients as well as which clients to display. The core information shown by user tracking reports includes:

- End user name
- End device MAC address
- End device hostname
- End device IP address
- If the end device is currently active on the network

- End device subnet
- Access device hostname/IP address
- Access device port
- Access device port VLAN
- Timestamp of when the end device connected to the network

Figure 5-6 shows a single user and end device in a generic user tracking report.

Figure 5-6 User and End Device in a Generic Tracking Report



User Name	MAC Address	Host Name	IP Address	Status	Subnet	Device Name	Port	VLAN	Last Seen
User1@mycompany.com	00-15-5d-98-4e-01	z-win7client-1	172.26.152.84	Active	172.26.152.0/24	z-3560r1-t	Gi0/14	VLAN0999	26 Feb 2011, 15:31:08 EST

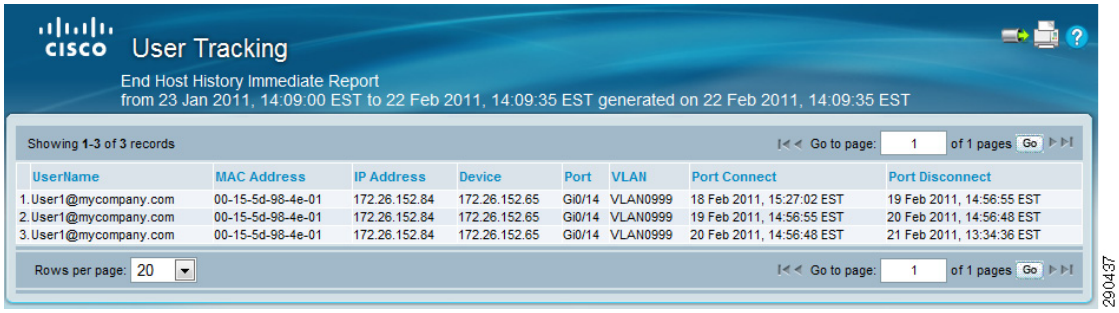
While Figure 5-6 shows only one user, reports may contain any number of users and devices.

User Tracking History

The User Tracking End Host History Report may be used to reference the history of end devices connecting and disconnecting from the network and users logging into and out of the network.

Figure 5-7 shows an example of historical tracking of an individual user, showing when and where they logged in and out.

Figure 5-7 Historical Tracking of an Individual User



Deployment Considerations

The following section is not intended to be a comprehensive installation guide, but rather a collection of significant implementation notes for User Tracking (End Device Tracking and End User Tracking) to supplement the core product documentation.

Product Documentation

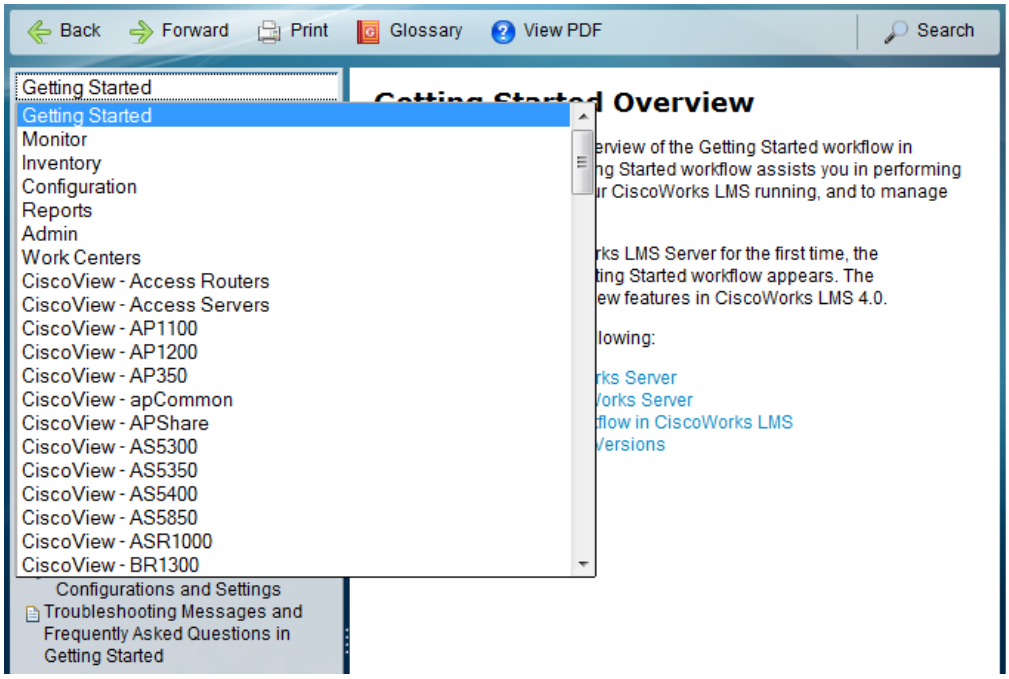
The most current implementation and configuration documentation can be found at: http://cisco.com/go/lms.

You should focus on the User Tracking sections of the *LMS 4.0 Administration Guide*.

In addition to documentation and information at http://cisco.com/go/lms, downloadable PDFs for all manuals and guides are available in the help section of LMS. Documentation is accessible after initial installation by clicking on the **Help** link in the top right corner of the Web interface.

The LMS help interface is shown in Figure 5-8. Click the white box **Getting Started** and a drop down box shows all the different documents. Click on a document, such as Admin, and then click **View PDF** at the top to download the entire *LMS 4.0 Administration Guide*.

Figure 5-8 LMS Help Interface



Firewall Port Configuration

Ensure that all incoming ports have exceptions in the operating system's firewall. Table 5-3 illustrates the critical ports that need to be open for LMS.

Table 5-3 LMS Critical Ports

Incoming Traffic	Default Port
Default HTTP port	1741
Default HTTPS port	443
Dynamic update SNMP traps	1431
All other SNMP traps	162
UTLite updates from clients	16236

Dynamic Updates for End Device Tracking

Dynamic updates require the access switch to send SNMP traps to LMS. Both global and interface level configuration must be completed on all access switches and their respective ports to enable dynamic updates.

At the interface level, SNMP traps must be enabled for any device connecting or disconnecting from the port.

Interface Configuration

```
snmp trap mac-notification change added
snmp trap mac-notification change removed
```

Global Configuration

```
snmp-server enable traps mac-notification change move threshold
snmp-server host [LMS server IP] [snmp string] udp-port 1431 mac-notification
mac address-table notification change
mac address-table notification mac-move
```

The default UDP port for SNMP traps related to User Tracking is 1431. This may seem to be a deviation from the standard port for SNMP traps, port 162, but there is a reason for using this port. LMS has two separate listeners, one for User Tracking-specific SNMP traps on port 1431 and one for all other SNMP traps on port 162. On the access devices, multiple "snmp-server" statements would be needed if LMS is to receive both User Tracking traps as well as other SNMP traps. LMS only needs to receive "mac-notification" traps for User Tracking.

UTLite Process for End User Tracking

End user tracking relies on the UTLite33.exe process to be run as a service on Windows clients. When a user logs into a domain, the executable is copied to the client and started from a domain login script. The script is:

```
REM UTLite33.exe options are:
REM    -domain <name>          NT/NDS domain name
REM    -host   <addr>          (Host IP address of ANI Server)
REM    -port   <num>           (listener port, default is 16236)
REM    -sleep  <num>           (default = 600, 10 minutes sync interval)
REM    -nds                    Will try to send NDS names
REM -sleep and -nds are optional parameters
REM
REM Copy UTLite33.exe file from domain controller to local client.
REM
REM if NOT EXIST %WINDIR%\UTLite33.exe
copy %0\..\UTLite33.exe %WINDIR%
REM
REM Specify the parameters below
REM
start %WINDIR%\UTLite33 -domain <domain> -host <ipaddress> -port 16236
REM
REM WINDIR is where NT system is installed, usually it is: C:\WINNT
REM
REM %0\.. is where UTLite33 is installed on the domain controller, it is
REM the same directory where the login scripts are usually kept. it is:
```

```
REM \WINNT\system32\Repl\Import\Scripts          (for NT) and
REM \\Novell-Server-name\SYS\public\Your-Folder  (for NDS)
REM
REM The client machine copies UTLite33.exe to its local WINDIR directory.
```

The default script copies the executable into the Windows directory. Permission issues may be encountered due to additional protections on this directory. Altering the script to copy and start the executable from an alternative location, such as a temp directory with %temp%, will not impact functionality.

In addition to setting the destination location, the domain and host must be set as well:

- Domain—The domain can be set to any text value and not necessarily the domain the user is using. This field may be used to differentiate users in the User Tracking Reporting to meet your needs.
- Host—The host is simply the LMS server IP address.

User Tracking Reporting

As noted earlier, there are many variations in generating User Tracking Reports, from individual users or devices to all users and devices on the network.

Custom reports may be created using the “Report Designer” in the reporting section of LMS. After creation, the location of the created reports may not be obvious. Custom reports reside in the following location.

Reports > Inventory > User Tracking

Click **User Tracking** and custom reports will be shown under all the standard User Tracking reports in the left menu. If the mouse is hovered over User Tracking instead of clicking it from the main navigation menu, all the standard User Tracking reports are shown, but not the custom reports.

Locations of User Tracking Features in LMS Interface

Table 5-4 Locations of User Tracking Features

User Tracking Feature	Location
Reporting	Reports > Inventory > User Tracking
Custom Report Creation	Reports > Report Designer > User Tracking
Acquisition Schedules	Admin > Collection Settings > User Tracking > Acquisition Schedule
Acquisition Settings and UTLite port	Admin > Collection Settings > User Tracking > Acquisition Settings
Dynamic Updates Listener enable and port	Admin > Collection Settings > User Tracking > Trap Listener Configuration
Manual Major Acquisition Execution	Admin > Collection Settings > User Tracking > Acquisition Action
Acquisition Info Summary	Admin > Collection Settings > User Tracking > Acquisition Info

User Tracking Utility Location

The User Tracking Utility must be downloaded from cisco.com. The location of the file is not obvious, however the following process should find it:

Go to http://www.cisco.com and then Support > Download Software.

Enter the following exactly as shown into the search box:

CiscoWorks Campus Manager 5.2

The manual path is:

Products > Network Management and Automation > Routing and Switching Management > CiscoWorks LAN Management Solution Products > CiscoWorks Campus Manager > CiscoWorks Campus Manager 5.2 > CiscoWorks Campus Manager User Tracking Utility

LMS User Tracking Summary

LMS User Tracking allows current and historical reporting of who is accessing the network, with what, from where, and when. The current and historical data available from LMS provides a single reference point for user and device tracking on the wired network.