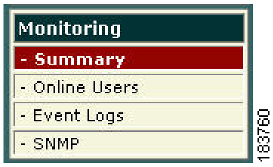
CHAPTER 15

Monitoring Online Users and Event Logs

This chapter describes the Monitoring module of Cisco NAC Appliance. Topics include:

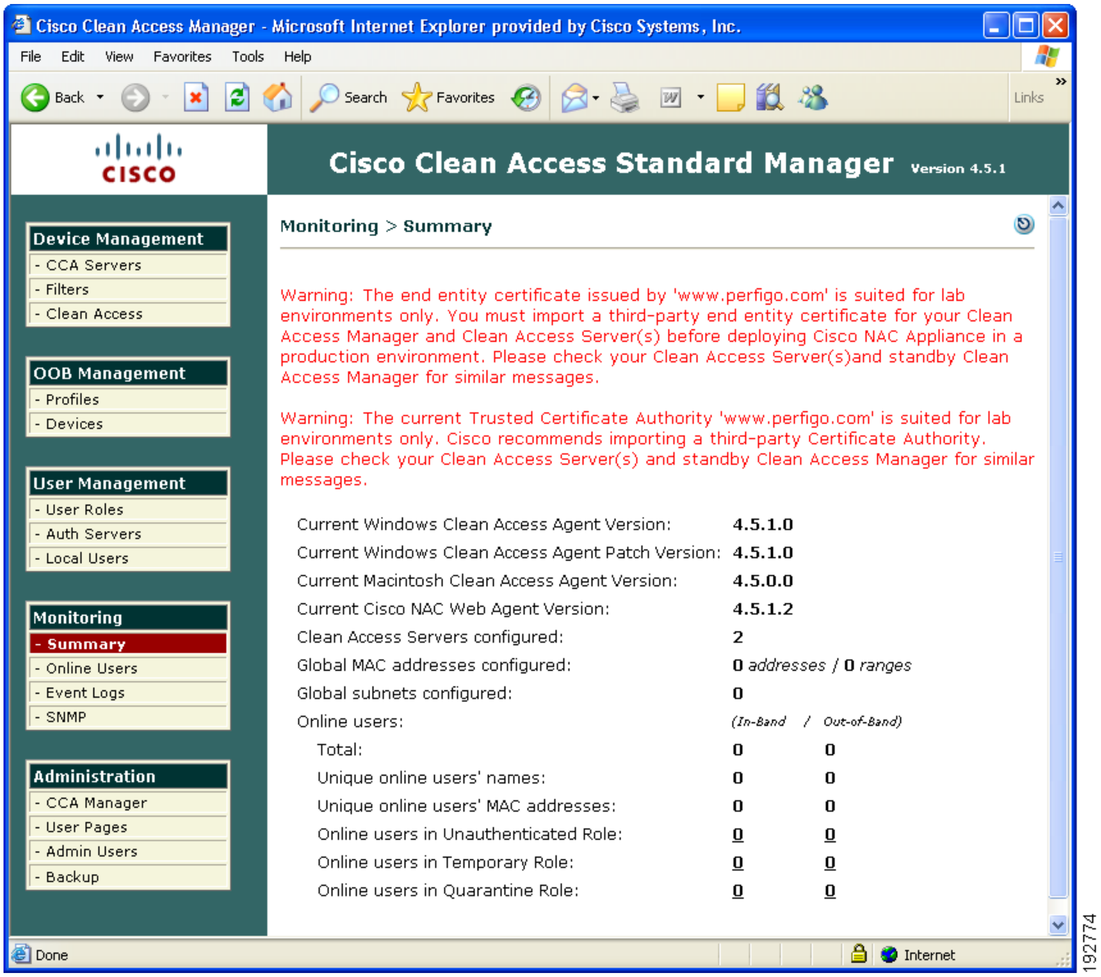
Overview

Figure 15-1 Monitoring Module



The Monitoring pages provide operational information for your deployment, including information on user activity, syslog events, network configuration changes. The Monitoring module also provides basic SNMP polling and alerts. The Monitoring Summary status page summarizes several important statistics, shown in Figure 15-2.

Figure 15-2 Monitoring > Summary Page



Monitoring > Summary

Warning: The end entity certificate issued by 'www.perfigo.com' is suited for lab environments only. You must import a third-party end entity certificate for your Clean Access Manager and Clean Access Server(s) before deploying Cisco NAC Appliance in a production environment. Please check your Clean Access Server(s)and standby Clean Access Manager for similar messages.

Warning: The current Trusted Certificate Authority 'www.perfigo.com' is suited for lab environments only. Cisco recommends importing a third-party Certificate Authority. Please check your Clean Access Server(s) and standby Clean Access Manager for similar messages.

Current Windows Clean Access Agent Version:	4.5.1.0	
Current Windows Clean Access Agent Patch Version:	4.5.1.0	
Current Macintosh Clean Access Agent Version:	4.5.0.0	
Current Cisco NAC Web Agent Version:	4.5.1.2	
Clean Access Servers configured:	2	
Global MAC addresses configured:	0 *addresses* / 0 *ranges*	
Global subnets configured:	0	
Online users:	*(In-Band /*	*Out-of-Band)*
Total:	0	0
Unique online users' names:	0	0
Unique online users' MAC addresses:	0	0
Online users in Unauthenticated Role:	0	0
Online users in Temporary Role:	0	0
Online users in Quarantine Role:	0	0

The page includes the information shown in Table 15-1.

Table 15-1 Monitoring > Summary Page

Item	Description
Current Windows Clean Access Agent Version	The current Windows version of the Clean Access Agent installed with the CAM software or manually uploaded (reflects the contents of the **Version** field).
Current Windows Clean Access Agent Patch Version	The latest Windows Clean Access Agent patch downloaded to the CAM and CAS(s) and available for client Auto-Upgrade.
Current Macintosh Clean Access Agent Version	The current version of the Mac OS X Clean Access Agent installed with the CAM software or manually uploaded (reflects the contents of the **Version** field).
Current Cisco NAC Web Agent Version	The current version of the Cisco NAC Web Agent installed with the CAM software or manually uploaded (reflects the contents of the **Version** field).
Clean Access Servers configured	The number of Clean Access Servers configured in the CAS management pages for the Clean Access Manager domain.

Table 15-1 Monitoring > Summary Page (continued)

Item	Description
Global MAC addresses configured (addresses/ranges)	The number of addresses and ranges currently in the MAC/IP device filter passthrough list. For details on MAC passthrough lists, see Global Device and Subnet Filtering, page 3-10.
Global Subnets configured	The number of subnet addresses currently in the subnet-based passthrough list. For more information, see Global Device and Subnet Filtering, page 3-10.
Online users (In-Band / Out-of-Band)	These entries list: • Total number of IB and/or OOB online user names • Total number of IB and/or OOB online MAC addresses • Number of IB and OOB online users per user role **Note** Per-role user tallies are links to the **Monitoring > Online Users > View Online Users** page. Clicking a link displays the IB or OOB online user list for the particular role.

Online Users List

Two **Online Users** lists are viewed from the **Monitoring > Online Users > View Online Users** tab:

- **In-Band Online Users**
  - Tracks in-band authenticated users logged into the network. In-band users with active sessions on the network are listed by characteristics such as IP address, MAC address (if available), authentication provider, and user role.
  - Removing a user from the In-Band Online Users list logs the user off of the in-band network.
- **Out-of-Band Online Users**
  - Tracks all authenticated out-of-band users that are on the Access VLAN (trusted network). Out-of-band users can be listed by Switch IP, Port, and Access VLAN, in addition to IP address, MAC address (if available), authentication provider, and user role.
  - Removing a user from the Out-of-Band Online Users list causes the VLAN of the port to be changed from the Access VLAN to the Authentication VLAN. You can additionally configure the Port profile to bounce the port (for Real-IP/NAT gateways). See Out-of-Band Users, page 15-6 and Out-of-Band Users, page 4-66 for details.

Both **Online Users** lists are based on the IP address of users. Note that:

- For Layer 2 deployments the **User MAC** address field is valid
- For Layer 3 deployments the **User MAC** address field is **not** valid (for example, 00:00:00:00:00:00)

Only the Certified Devices List is based on client MAC addresses, and therefore the Certified Devices List never applies to users in Layer 3 deployments.

For Out-of-Band deployments, OOB users always display first in the In-Band Online Users list, then in the Out-of-Band Online Users list. When user traffic is coming from a controlled port of a managed switch, the user shows up first in the In-Band Online Users list during the authentication process, then is moved to the Out-of-Band Online Users list after the user is authenticated and moved to the Access VLAN.

Finally, the **Display Settings** tab let you choose which user characteristics are displayed on each respective **Online Users** page.

Note When a user device is connecting to Cisco NAC Appliance from behind a VPN3000/ASA device, the MAC address of the first physical adapter that is available to the CAS/CAM is used to identify the user on the Online Users list. This may not necessarily be the adapter with which the user is connecting to the network. Users should **disable** the wireless interface of their machines when connecting to the network using the wired (Ethernet card) interface.

Interpreting Active Users

Once logged onto the Cisco NAC Appliance network, an active user session persists until one of the following events occurs:

- The user logs out of the network through the browser logout page or Clean Access Agent/Cisco NAC Web Agent logout.

  Once on the network, users can remain logged on after a computer shutdown/restart. A user can log out of the network using the web logout page or Clean Access Agent/Cisco NAC Web Agent logout.

- The Clean Access Agent/Cisco NAC Web Agent user logs off Windows or shuts down Windows machine.

  You can configure the CAM and Agent to log off In-Band users only from the Clean Access system when the user logs off from the Windows domain (i.e. **Start > Shutdown > Log off current user**) or shuts down the machine (**Start > Shutdown > Shutdown machine**).

- An administrator manually drops the user from the network.

  The **Monitoring > Online Users > View Online Users** page (IB or OOB) can be used to drop users from the network, without deleting their clients from the Certified Devices List.

- The session times out using the Session Timer.

  The Session Timer works the same way for multi-hop L3 (IB) deployments as for L2 (IB or OOB) deployments and is set in **User Management > User Roles> Schedule > Session Timer**. It is set per user role, and logs out any user in the selected role from the network after the configured time has elapsed. For details, see Configure Session Timer (per User Role), page 9-17.

- The CAS determines that the user is no longer connected using the Heartbeat Timer and the CAM terminates the session.

  The Heartbeat Timer applies to L2 IB deployments only and is set for all users regardless of role. It can be set globally for all Clean Access Servers using the form **User Management > User Roles> Schedule > Heartbeat Timer**, or for a specific Clean Access Server using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Heartbeat Timer**. For details, see Configure Heartbeat Timer (User Inactivity Timeout), page 9-17.

  The Heartbeat Timer will not function in L3 deployments, and does not apply to OOB users. However, note that the HeartBeat Timer will work if the CAS is the first hop behind the VPN concentrator. This is because the VPN concentrator responds to the ARP queries for the IP addresses of its current tunnel clients.

- The Certified Device list is cleared (automatically or manually) and the user is removed from the network.

The Certified Devices List applies to L2 (IB or OOB) deployments only and can be scheduled to be cleared automatically and periodically using the global Certified Devices timer form (**Device Management > Clean Access > Certified Devices > Timer**). You can manually clear the certified devices for a specific Clean Access Server from the Certified Devices List using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Filters > Clean Access > Certified Devices,** or manually clear the Certified Device list across all Clean Access Servers using the global form **Device Management > Clean Access > Certified Devices**. For details, see Manage Certified Devices, page 10-30.

Keep in mind that the Certified Devices List will not display remote VPN/L3 clients (since these sessions are IP-based rather than MAC address-based).

- SSO and Auto-Logout are configured for the VPN concentrator, and the user disconnects from the VPN.

  With Auto Logout enabled, when the user disconnects from the VPN client, the user is automatically removed from the Online Users list (In-Band).

  Note that when SSO is configured for multi-hop L3 VPN concentrator integration, if the user's session on the CAS times out but the user is still logged in on the VPN concentrator, the user will be able to log back into the CAS without providing a username/password.

Note Whether the CAS or another server is used for DHCP, if a user's DHCP lease expires, the user remains on the Online Users list (in-band or out-of-band). When the lease expires, the client machine will try to renew the lease.

See also Configure User Session and Heartbeat Timeouts, page 9-15 and Out-of-Band Users, page 4-66 for additional details.

View Online Users

The **View Online Users** tab provides two links for the two online users lists: **In-Band** and **Out-of-Band**.

By default, **View Online User** pages display the login user name, IP and MAC address (if available), provider, and role of each user. For information on selecting the column information to display, such as OS version, or for out-of-band users: switch port, see Display Settings, page 15-10.

A *green* background for an entry indicates a user device accessing the Clean Access network in a temporary role: either a Quarantine role or the Agent Temporary role.

A *blue* background for an entry indicates a user device accessing the Clean Access network in a restricted network access role.

A device listed on the **View Online Users** page but not in the Clean Access **Certified Devices List** generally indicates the device is in the process of certification.

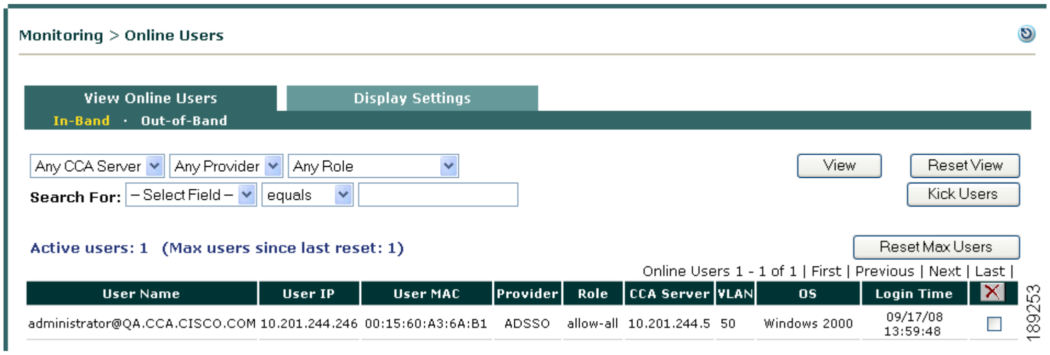
In-Band Users

Clicking the **In-Band** link brings up the **View Online Users** page for in-band users (Figure 15-3). The In-Band Online Users list tracks the in-band users logged into the Clean Access network.

The Clean Access Manager adds a client IP and MAC address (if available) to this list after a user logs into the network either through web login or the Clean Access Agent/Cisco NAC Web Agent.

Removing a user from the Online Users list logs the user off the in-band network.

Figure 15-3 View Online Users Page—In-Band



Active users: 1 (Max users since last reset: 1)

Online Users 1 - 1 of 1 | First | Previous | Next | Last |

User Name	User IP	User MAC	Provider	Role	CCA Server	VLAN	OS	Login Time	☒
administrator@QA.CCA.CISCO.COM	10.201.244.246	00:15:60:A3:6A:B1	ADSSO	allow-all	10.201.244.5	50	Windows 2000	09/17/08 13:59:48	□

Note For AD SSO users, the **Provider** field displays **`AD_SSO`**, and the **User/User Name** field lists both the username and domain of the user (for example, **`user1@domain.name.com`**.) on the **Online Users** and **Certified Devices** pages.

Out-of-Band Users

Clicking the **Out-of-Band** link brings up the **View Online Users** page for out-of-band users (Figure 15-4).

The Out-of-Band Online Users list tracks all out-of-band authenticated users that are on the Access VLAN (on the trusted network). The CAM adds a user IP address to the Out-of-Band Online Users list after a client is switched to the Access VLAN.

Note **The "User IP" of Out-of-Band online users will be the IP address of the user on the Authentication VLAN. By definition CCA does not track users once they are on the Access VLAN; therefore OOB users are tracked by the Auth VLAN IP address they have while in the CCA network.**

When a user is removed from the Out-of-Band Online Users list, the following typically occurs:

1. The CAM bounces the switch port (off and on).
2. The switch resends SNMP traps to the CAM.
3. The CAM changes the VLAN of the port based on the configured Port Profile associated with this controlled port.

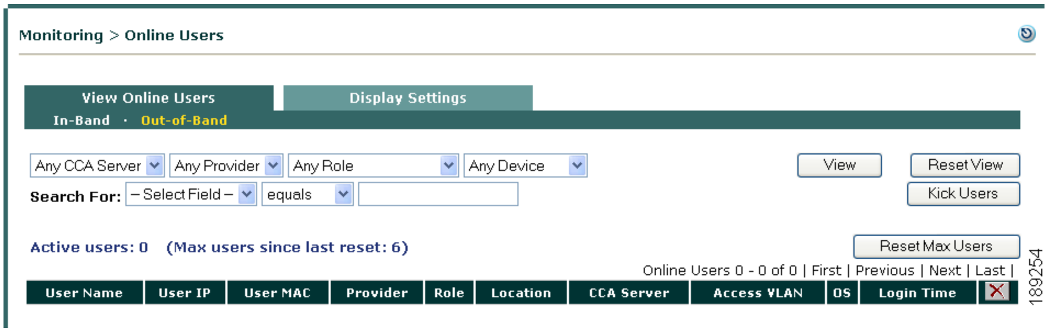
Note Removing an OOB user from the Certified Devices List also removes the user from Out-of-Band Online Users list and changes the port from the Access VLAN to the Auth VLAN.

Note When the “**Remove Out-of-Band online user without bouncing port**” option is checked for the Port Profile, for OOB Virtual Gateways, the switch port will not be bounced when:

- Users are removed from the Out-of-Band Online Users List, or
- Devices are removed from the Certified Devices list

Instead, the port Access VLAN will be changed to the Authentication VLAN (see Add Port Profile, page 4-29 for details).

Figure 15-4 View Online Users Page—Out-of-Band



Active users: 0 (Max users since last reset: 6)

Note For AD SSO users, the **Provider** field displays `AD_SSO`, and the **User/User Name** field lists both the username and domain of the user (for example, `user1@domain.name.com`.) on the **Online Users** and **Certified Devices** pages.

For more details, see Chapter 4, “Switch Management: Configuring Out-of-Band Deployment.”

Table 15-2 describes the search criteria, information/navigation elements, and options for removing user.s from the online users pages. Note that clicking a column heading sorts entries on the page by the column.

Table 15-2 View Online Users Page Controls

Item	Description
User Name	The user name used for login is displayed.

Table 15-2 View Online Users Page Controls

Item		Description
Search Criteria:	**CCA Server**	• Any Clean Access Server • <specific CAS IP address>
	Provider	• Any Provider • <specific authentication provider>
	Role	• Any Role • Unauthenticated Role • Temporary Role • Quarantine Role • <specific Role>
	Location	• Any Switch or Wireless LAN Controller • <specific switch/WLC IP address>
	Select Field	• User Name • IP Address • MAC Address
	Operator	**equals**: Search text value must be an exact match for this operator **starts with:** **ends with:** **contains**:
	Search Text	Enter the value to be searched using the operator selected.
Controls:	**View**	After selecting the search criteria, click **View** to display the results. You can view users by CAS, provider, user role, user name, IP address, MAC address (if available), or switch (OOB only).
	Reset View	Resets to the default view (with search criteria reset to "Any")
	Kick Users	**Clicking Kick Users** terminates all user sessions filtered through the search criteria across the number of applicable pages. Users can be selectively dropped from the network by any of the search criteria used to **View** users. The "filtered users indicator" shown in Figure 15-3 displays the total number of filtered users that will be terminated when **Kick Users** is clicked.
	Reset Max Users	Resets the maximum number of users to the actual number of users displayed in the "Active users:" status field (Figure 15-3)
	Kick User	You can remove as many users as are shown on the **page** by selecting the checkbox next to each user and clicking the Kick User button.
Navigation:	**First/Previous/Next/Last**	These navigation links allow you to page through the list of online users. A maximum of 25 entries is displayed per page.

View Users by Clean Access Server, Authentication Provider, or Role

1. From the **View Online Users** page, select a specific Clean Access Server, or leave the first field as **Any CCA Server**.
2. Select a specific authentication provider, or leave as **Any Provider**.
3. Select a specific user role, or leave as **Any Role**.
4. Click **View** to display users by Clean Access Server, provider, role or any combination of the three.

Search by User Name, IP, or MAC Address

1. In the **Select Field** dropdown menu next to **Search For:**, select **User Name** or **IP Address** or **MAC Address**.
2. Select one of the four operators: **starts with**, **ends with**, **contains**, **exact match**.
3. Enter the text to be searched in the **Search For:** text field. If using the **exact match** operator, only the exact match for the search text entered is returned.
4. Click **View** to display results.

Log Users Off the Network

Clicking Kick Users terminates all user sessions filtered through the search criteria across the number of applicable pages. (Note that a maximum of 25 entries is displayed per page.) You can selectively remove users from the network by any of the search criteria used to **View** users. The “filtered users indicator” shown in Figure 15-3 displays the total number of filtered user sessions that will be terminated when you click the **Kick Users** button.

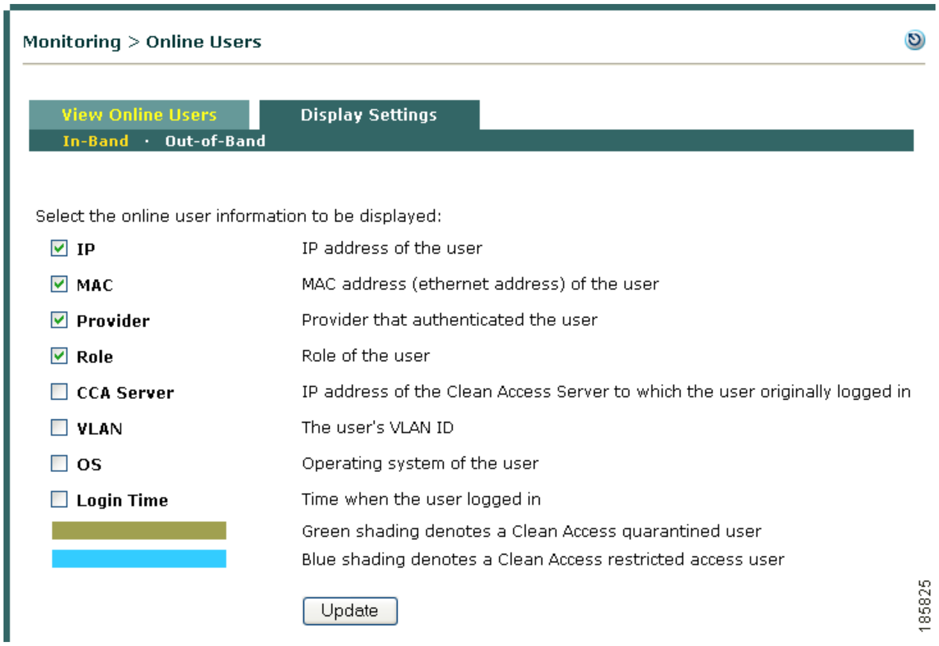
1. Go to **Monitoring > Online Users > View Online Users**.
2. To terminate user sessions either:
   - Drop all users (filtered through search criteria) from the network by clicking **Kick Users**
   - Drop individual users by selecting the checkbox next to each user and clicking the **Kick User** button.

Note that removing a user from the online users list (and the network) does not remove the user from the **Certified Devices List**. However, dropping a user from the Certified Devices List also logs the user off the network. See Certified Devices List, page 10-9 for further details.

Display Settings

Figure 15-5 shows the **Display Settings** page for in-band users.

Figure 15-5   Display Settings—In-Band



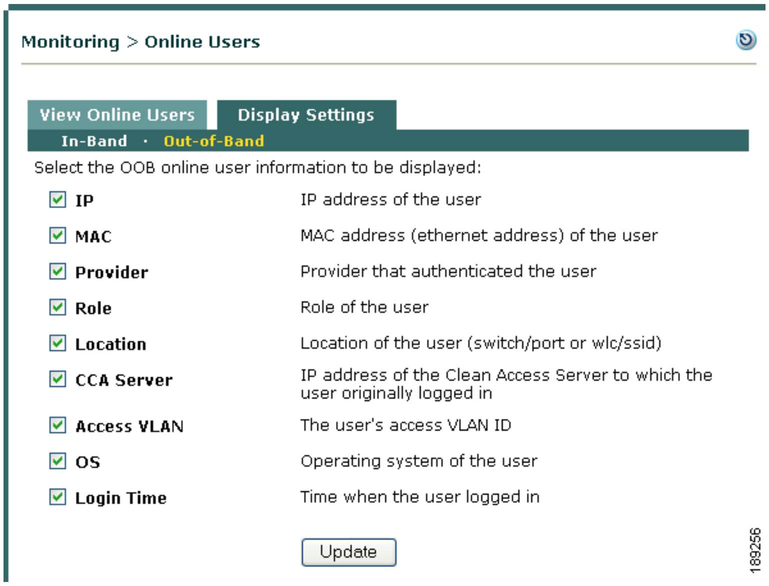
Select the online user information to be displayed:

☑ **IP**	IP address of the user
☑ **MAC**	MAC address (ethernet address) of the user
☑ **Provider**	Provider that authenticated the user
☑ **Role**	Role of the user
☐ **CCA Server**	IP address of the Clean Access Server to which the user originally logged in
☐ **VLAN**	The user's VLAN ID
☐ **OS**	Operating system of the user
☐ **Login Time**	Time when the user logged in
🟩	Green shading denotes a Clean Access quarantined user
🟦	Blue shading denotes a Clean Access restricted access user

Note **Role**—the role assigned to the user upon login.

Figure 15-6 shows the **Display Settings** page for out-of-band users.

Figure 15-6 Display Settings—Out-of-Band



Select the OOB online user information to be displayed:

☑ **IP**	IP address of the user
☑ **MAC**	MAC address (ethernet address) of the user
☑ **Provider**	Provider that authenticated the user
☑ **Role**	Role of the user
☑ **Location**	Location of the user (switch/port or wlc/ssid)
☑ **CCA Server**	IP address of the Clean Access Server to which the user originally logged in
☑ **Access VLAN**	The user's access VLAN ID
☑ **OS**	Operating system of the user
☑ **Login Time**	Time when the user logged in

To choose what information is displayed on the View Online Users page:

1. Click the **Display Settings** tab.
2. Select the check box next to an item to display it in the list.
3. Click **Update**.
4. Click the **View Online Users** tab to see the desired settings displayed.

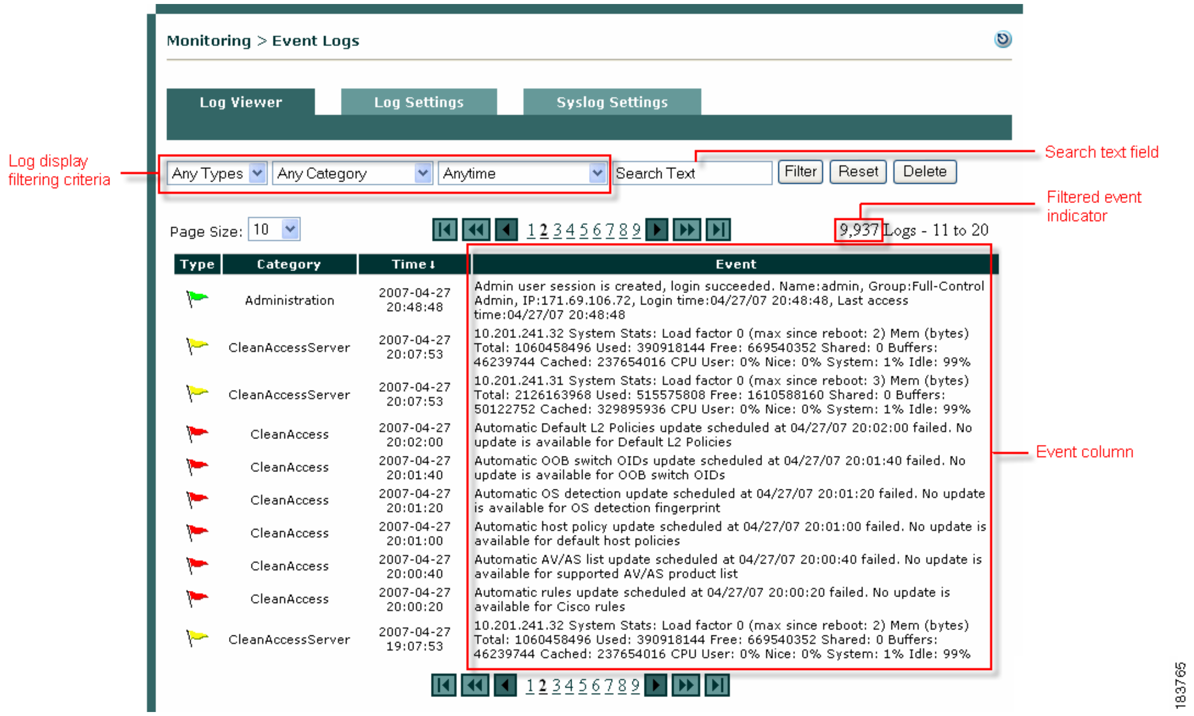
Interpreting Event Logs

Click the **Event Logs** link in the **Monitoring** module to view syslog-based event logs in the admin console. There are three Event Logs tabs: **Log Viewer**, **Logs Settings**, and **Syslog Settings**.

View Logs

Figure 15-7 shows the Log Viewer pane.

Figure 15-7 Log Viewer Pane



Log display filtering criteria

Search text field

Filtered event indicator

Event column

9,937 Logs - 11 to 20

Type	Category	Time	Event
🟩	Administration	2007-04-27 20:48:48	Admin user session is created, login succeeded. Name:admin, Group:Full-Control Admin, IP:171.69.106.72, Login time:04/27/07 20:48:48, Last access time:04/27/07 20:48:48
🟨	CleanAccessServer	2007-04-27 20:07:53	10.201.241.32 System Stats: Load factor 0 (max since reboot: 2) Mem (bytes) Total: 1060458496 Used: 390918144 Free: 669540352 Shared: 0 Buffers: 46239744 Cached: 237654016 CPU User: 0% Nice: 0% System: 1% Idle: 99%
🟨	CleanAccessServer	2007-04-27 20:07:53	10.201.241.31 System Stats: Load factor 0 (max since reboot: 3) Mem (bytes) Total: 2126163968 Used: 515575808 Free: 1610588160 Shared: 0 Buffers: 50122752 Cached: 329895936 CPU User: 0% Nice: 0% System: 1% Idle: 99%
🟥	CleanAccess	2007-04-27 20:02:00	Automatic Default L2 Policies update scheduled at 04/27/07 20:02:00 failed. No update is available for Default L2 Policies
🟥	CleanAccess	2007-04-27 20:01:40	Automatic OOB switch OIDs update scheduled at 04/27/07 20:01:40 failed. No update is available for OOB switch OIDs
🟥	CleanAccess	2007-04-27 20:01:20	Automatic OS detection update scheduled at 04/27/07 20:01:20 failed. No update is available for OS detection fingerprint
🟥	CleanAccess	2007-04-27 20:01:00	Automatic host policy update scheduled at 04/27/07 20:01:00 failed. No update is available for default host policies
🟥	CleanAccess	2007-04-27 20:00:40	Automatic AV/AS list update scheduled at 04/27/07 20:00:40 failed. No update is available for supported AV/AS product list
🟥	CleanAccess	2007-04-27 20:00:20	Automatic rules update scheduled at 04/27/07 20:00:20 failed. No update is available for Cisco rules
🟨	CleanAccessServer	2007-04-27 19:07:53	10.201.241.32 System Stats: Load factor 0 (max since reboot: 2) Mem (bytes) Total: 1060458496 Used: 390918144 Free: 669540352 Shared: 0 Buffers: 46239744 Cached: 237654016 CPU User: 0% Nice: 0% System: 1% Idle: 99%

The **Log Viewer** tab includes the following information:

- System statistics for Clean Access Servers (generated every hour by default)
- User activity, with user logon times, log-off times, failed logon attempts, and more.
- Network configuration events, including changes to the MAC or IP passthrough lists, and addition or removal of Clean Access Servers.
- Device management events (for OOB), including when linkdown traps are received, and when a port changes to the Auth or Access VLAN.
- Changes or updates to Clean Access checks, rules, and Supported AV/AS Product List.
- Changes to Clean Access Server DHCP configuration.

System statistics are generated for each CAS managed by the Clean Access Manager every hour by default. See Configuring Syslog Logging, page 15-17 to change how often system checks occur.

Note The most recent events appear first in the Events column.

Table 15-3 describes the navigation, searching capabilities, and actual syslog displayed on the Log Viewer page.

Table 15-3 Log Viewer Page

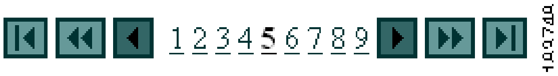
	Column	Description
Navigation	**First Page/Previous Page/ Previous Entry/Specific Page/Next Entry/Next Page/Last Page**	These navigation links page through the event log. The most recent events appear first in the Events column. The **Last** link shows you the oldest events in the log. 
	Page Size	The number of log entries displayed in the window. (You can specify 10, 25, or 100 entries per page.)
	Column	Click a column heading (e.g. Type or Category) to sort the Event log by that column.

Table 15-3 Log Viewer Page (continued)

	Column	Description
Search criteria	**Type**	Search by Type column criteria (then click **Filter**): • Any Type • Failure • Information • Success
	Category	Search by Category column criteria (then click **Filter**): • Authentication [1] • Administration • Client • Clean Access Server • Clean Access • SW_Management (if OOB is enabled) • DHCP • Guest Registration • SSL Communication • Miscellaneous
	Time	Search by the following Time criteria (then click **Filter**): • Within one hour • Within one day • Within two days • Within one week • Anytime • One hour ago • One day ago • Two days ago • One week ago
	Search in log text	Type desired search text and click **Filter**
Controls	**Filter**	After selecting the desired search criteria, click **Filter** to display the results.
	Reset	Clicking **Reset** restores the default view, in which logs within one day are displayed.
	Delete	Clicking Delete removes the events filtered through the search criteria across the number of applicable pages. Clicking Delete removes filtered events from Clean Access Manager storage. Otherwise, the event log persists through system shutdown. Use the filter event indicator shown in Figure 15-7 on page 15-12 to view the total number of filtered events that are subject to being deleted.

Table 15-3 Log Viewer Page (continued)

	Column	Description
Status Display	**Type**	- Red flag (⚑) = Failure; indicates error or otherwise unexpected event. - Green flag (⚑) = Success; indicates successful or normal usage event, such as successful login and configuration activity. - Yellow flag (⚑) = Information; indicates system performance information, such as load information and memory usage.
	Category	Indicates the module or system component that initiated the log event. (For a list, see Category, page 15-14.) Note that system statistics are generated for each Clean Access Server managed by the Clean Access Manager every hour by default.
	Time	Displays the date and time (hh:mm:ss) of the event, with the most recent events appearing first in the list.
	Event	Displays the event for the module, with the most recent events listed first. See Table 15-4 on page 15-16 for an example of Clean Access Server event.

[1] Authentication-type entries may include the item "Provider: <provider type>, Access point: N/A, Network: N/A." To continue to provide support for the EOL'ed legacy wireless client (if present and pre-configured in the Manager), the "Access point: N/A, Network: N/A" fields provide AP MAC and SSID information respectively for the legacy client.

Event Log Example

Table 15-4 explains the following typical Clean Access Server health event example:

```
CleanAccessServer 2007-04-05 09:03:31 10.201.15.2 System Stats: Load factor 0 (max
since reboot: 2) Mem (bytes) Total: 528162816 Used: 295370752 Free: 232792064 Shared:
0 Buffers: 41537536 Cached: 179576832 CPU User: 0% Nice: 0% System: 1% Idle: 99%
```

Table 15-4 Event Column Fields

Value	Description
`CleanAccessServer`	A Clean Access Server is reporting the event
2007-04-05 09:03:31	Date and time of the event
10.201.15.2	IP address of reporting Clean Access Server
`System Stats:`	System statistics are generated for each Clean Access Server managed by the Clean Access Manager every hour by default.
`Load factor 0`	Load factor is a number that describes the number of packets waiting to be processed by the Clean Access Server (that is, the current load being handled by the CAS). When the load factor grows, it is an indication that packets are waiting in the queue to be processed. If the load factor exceeds 500 for any consistent period of time (e.g. 5 minutes), this indicates that the Clean Access Server has a steady high load of incoming traffic/packets. You should be concerned if this number increases to 500 or above.
`(max since reboot: <n>)`	The maximum number of packets in the queue at any one time (i.e. the maximum load handled by the Clean Access Server).
Mem Total: 528162816 bytes	These are the memory usage statistics. There are 6 numbers shown here: total memory, used memory, free memory, shared memory, buffer memory, and cached memory.
`Used:` 295370752 `bytes`	
`Free:` 232792064 `bytes`	
`Shared: 0 bytes`	
`Buffers:` 41537536 `bytes`	
`Cached:` 179576832 `bytes`	
`CPU User: 0%`	These numbers indicate CPU processor load on the hardware, in percentages. These four numbers indicate time spent by the system in user, nice, system, and idle processes. **Note** Time spent by the CPU in system process is typically < 90% on a Clean Access Server. This indicates a healthy system.
`Nice: 0%`	
`System: 1%`	
`Idle: 99%`	

Limiting the Number of Logged Events

The event log threshold is the number of events to be stored in the Clean Access Manager database. The maximum number of log events kept on the CAM, by default, is 100,000. You can specify an event log threshold of up to 200,000 entries to be stored in the CAM database at a time. The event log is a circular log. The oldest entries will be overwritten when the log passes the event log threshold.

To change the maximum number of events:

1. Click the **Logs Setting** tab in the **Monitoring > Event Logs** pages.
2. Type the new number in the **Maximum Event Logs** fields.
3. Click **Update**.

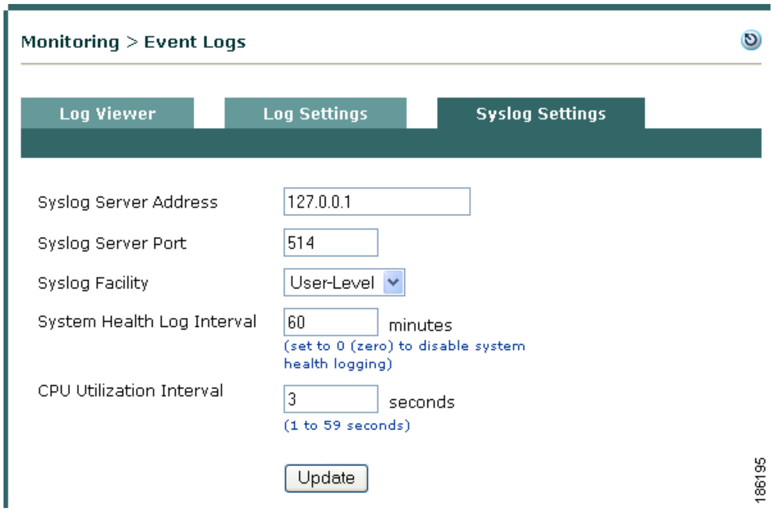
Configuring Syslog Logging

System statistics are generated for each Clean Access Server managed by the Clean Access Manager every hour by default. By default, event logs are written to the CAM. You can redirect CAM event logs to another server (such as your own syslog server).

Additionally, you can configure how often you want the CAM to log system status information by setting the value in the **Syslog Health Log Interval** field (default is **60** minutes).

To configure Syslog logging:

Step 1 Go to **Monitoring > Event Logs > Syslog Settings**.



Monitoring > Event Logs

Syslog Server Address: 127.0.0.1

Syslog Server Port: 514

Syslog Facility: User-Level

System Health Log Interval: 60 minutes (set to 0 (zero) to disable system health logging)

CPU Utilization Interval: 3 seconds (1 to 59 seconds)

Step 2 In the **Syslog Server Address** field, type the IP address of the Syslog server (default is **127.0.0.1**).

Step 3 In the **Syslog Server Port** field, type the port for the Syslog server (default is **514**).

Step 4 Specify a **Syslog Facility** from the dropdown list. This setting enables you to optionally specify a different Syslog facility type for Syslog messages originating from the CAM. You can use the default “User-Level” facility type, or you can assign any of the “local use” Syslog facility types defined in the Syslog RFC (“Local use 0” to “Local use 7”). This feature gives you the ability to differentiate Cisco Clean Access Syslog messages from other “User-Level” Syslog entries you may already generate and direct to your Syslog server from other network components.

Step 5 In the **System Health Log Interval** field, specify how often you want the CAM to log system status information, in minutes (default is **60** minutes). This setting determines how frequently CAS statistics are logged in the event log.

Step 6 In the **CPU Utilization Interval** field, specify how often, in seconds, you want the CAM to record CPU utilization statistics. You can configure the CAM to record CPU status information up to nearly every minute and the default is every **3** seconds.

Step 7 Click the **Update** button to save your changes.

Note After you set up your Syslog server in the CAM, you can test your configuration by logging off and logging back into the CAM admin console. This will generate a Syslog event. If the CAM event is not seen on your Syslog server, make sure that the Syslog server is receiving UDP 514 packets and that they are not being blocked elsewhere on your network.

Note You can only forward to one syslog server. You can have that syslog server forward to another if required.

Cisco NAC Appliance Log Files

Table 15-5 lists common Clean Access Manager and Clean Access Server logs in Cisco NAC Appliance.

Table 15-5 Cisco NAC Appliance Log Files

File	Description
`/var/log/messages`	Startup
`/perfigo/control/tomcat/logs/nac_manager.log`	Perfigo service logs for release 4.5 and later [1,2]
`/perfigo/control/data/details.html` `/perfigo/control/data/upgrade.html`	CAM upgrade logs
`/var/nessus/logs/nessusd.messages`	Nessus plugin test logs
`/perfigo/control/apache/logs/*`	SSL (certificates), Apache error logs
`/perfigo/control/tomcat/logs/catalina.out`	Tomcat initialization logs
`/var/log/ha-log`	High availability logs (both CAM and CAS)
`/var/log/dhcplog`	DHCP relay, DHCP logs (CAS)
`/perfigo/access/data/details.html` `/perfigo/access/data/upgrade.html`	CAS upgrade logs
`/perfigo/access/tomcat/logs/nac_server.log`	Certificate-related CAM/CAS connection errors (CAS)

[1] Device Management events for notifications received by the CAM from switches are written only to the logs on the file system (**/perfigo/control/tomcat/logs/nac_manager.log**). These events are written to disk only when the log level is set to INFO or finer.

[2] Perfigo service log files in previous releases of Cisco NAC Appliance reside in the **/perfigo/logs/perfigo-log0.log.*** or **/tmp/perfigo-log0.log.*** (pre-release 3.5(5)) directory. For these older logs, 0 instead of * shows the most recent log.

Log File Sizes

- There are 10 logs with a maximum size of 20 MB for the **/perfigo/control/tomcat/logs/nac_manager.log** log file.
- There are 20 logs with maximum size of 20 MB for each log file under /perfigo/(control | access)/apache/logs.

For additional details see also:

- Support Logs, page 16-42
- Certificate-Related Files, page 16-23.
- Backing Up the CAM Database, page 16-56

SNMP

You can configure the Clean Access Manager to be managed/monitored by an SNMP management tool (such as HP OpenView). This feature provides minimal manageability using SNMP (v1). It is expected that future releases will have more information/actions exposed via SNMP.

You can configure the Clean Access Manager for basic SNMP polling and alerting through **Monitoring > SNMP**. Note that SNMP polling and alerts are disabled by default. Clicking the **Enable** button under **Monitoring > SNMP** activates the following features:

- SNMP Polling—If an SNMP `rocommunity` ("Read-only community") string is specified, the Clean Access Manager will respond to `snmpget` and `snmpwalk` requests with the correct community string.
- SNMP Traps—The Clean Access Manager can be configured to send traps by adding trap sinks. A *trap sink* is any computer configured to receive traps, typically a management box. All traps sent are version 1 (v1) traps. A copy of each trap will be sent to each trapsink.

When enabled, the SNMP module monitors the following processes:

- SSH Daemon
- Postgres Database
- Clean Access Manager
- Apache Web Server

The Clean Access Manager also sends traps in the following cases:

- When the Clean Access Manager comes online.
- When the Clean Access Manager shuts down.
- When the Clean Access Manager gains or loses contact with any Clean Access Servers it manages.
- When the SNMP service starts (a Cold Start Trap is sent).

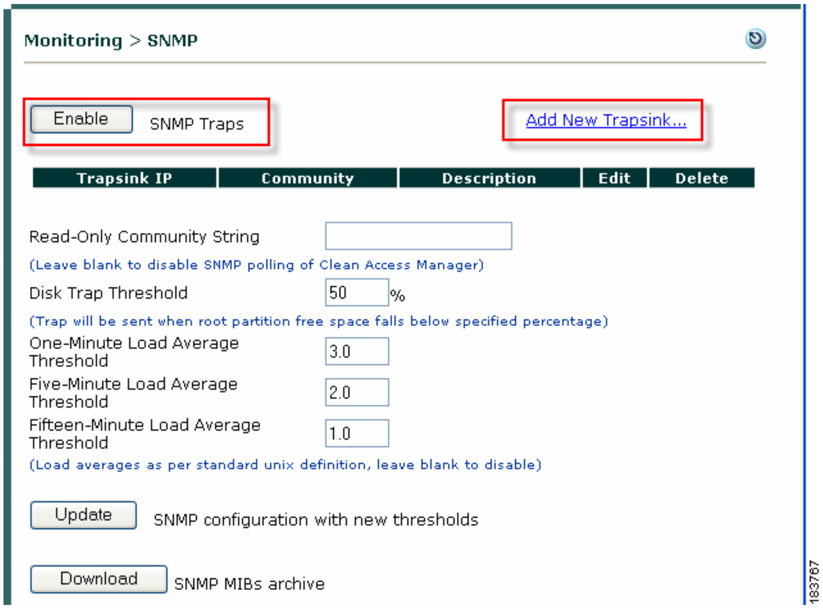
This section describes the following:

- Enable SNMP Polling/Alerts
- Add New Trapsink

Enable SNMP Polling/Alerts

1. Go to **Monitoring > SNMP** to bring up the SNMP configuration page (Figure 15-8).

Figure 15-8 Monitoring > SNMP Page



Monitoring > SNMP

Enable SNMP Traps

Add New Trapsink...

Trapsink IP	Community	Description	Edit	Delete

Read-Only Community String:
(Leave blank to disable SNMP polling of Clean Access Manager)

Disk Trap Threshold: 50 %
(Trap will be sent when root partition free space falls below specified percentage)

One-Minute Load Average Threshold: 3.0

Five-Minute Load Average Threshold: 2.0

Fifteen-Minute Load Average Threshold: 1.0
(Load averages as per standard unix definition, leave blank to disable)

Update SNMP configuration with new thresholds

Download SNMP MIBs archive

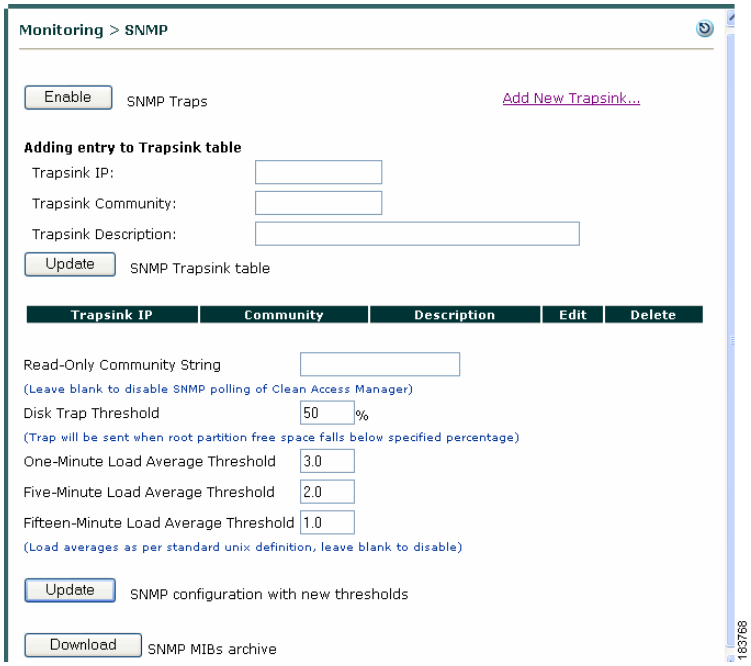
2. Click the **Enable** button to activate SNMP polling and SNMP traps.
3. Specify values for the following fields:
   - **Read-Only Community String:**
     Specify a string to enable the Clean Access Manager to respond to snmpget and snmpwalk requests with the correct community string.
     Leave blank to disable all Clean Access Manager responses to SNMP polling of the Clean Access Manager.
   - **Disk Trap Threshold%:** (default is 50%)
     A trap will be sent when root partition free space falls below specified percentage.
   - **One-Minute Load Average Threshold:** (default is 3.0)
     A trap will be sent when the one-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
   - **Five-Minute Load Average Threshold:** (default is 2.0)
     A trap will be sent when the 5-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
   - **Fifteen-Minute Load Average Threshold:** (default is 1.0)
     A trap will be sent when the 15-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
4. Click **Update** to update the SNMP configuration with new thresholds.
5. Click **Download** to download the SNMP MIB archive in .tar.gz form.

Add New Trapsink

The Clean Access Manager can be configured to send traps by adding trap sinks. All traps sent are version 1 (v1) traps. A copy of each trap will be sent to each trapsink.

1. Click the **Add New Trapsink** link in the upper-right-hand corner of the pane to bring up the Add New Trapsink form.
2. Enter a **Trapsink IP**.
3. Enter a **Trapsink Community** string.
4. Enter an optional **Trapsink Description**.
5. Click **Update** to update the SNMP Trapsink table.

Figure 15-9 Add New Trapsink



Monitoring > SNMP

Enable SNMP Traps

Add New Trapsink...

Adding entry to Trapsink table

Trapsink IP:

Trapsink Community:

Trapsink Description:

Update SNMP Trapsink table

Trapsink IP	Community	Description	Edit	Delete

Read-Only Community String

(Leave blank to disable SNMP polling of Clean Access Manager)

Disk Trap Threshold 50 %

(Trap will be sent when root partition free space falls below specified percentage)

One-Minute Load Average Threshold 3.0

Five-Minute Load Average Threshold 2.0

Fifteen-Minute Load Average Threshold 1.0

(Load averages as per standard unix definition, leave blank to disable)

Update SNMP configuration with new thresholds

Download SNMP MIBs archive

Once trapsink configuration is complete, the Clean Access Manager will send DISMAN-EVENT style traps which refer to UCD table entries. The Clean Access Manager also sends traps if the root partition falls below a configured amount of space remaining (which defaults to 50%), and if the CPU load is above the configured amount for 1, 5 or 15 minutes.

A trap will contain the following contents:

Trap Contents	Description
Type: Enterprise-Specific(1)	
SNMP Trap OID (1.3.6.1.6.3.1.1.4.1.0)	Set to DISMAN-EVENT-MIB 2.0.1 (1.3.6.1.2.1.88.2.0.1)

Trap Contents	Description
The contents of a DISMAN mteObjectsEntry:	
mteHotTrigger (OID 1.3.6.1.2.1.88.2.1.1)	Generally: “process table” for processes “laTable” for load average alerts “dskTable” for disk capacity alerts “memory” for virtual memory alerts
mteHotTargetName (OID 1.3.6.1.2.1.88.2.1.2)	Always blank.
mteHotContextName (OID 1.3.6.1.2.1.88.2.1.3)	Always blank.
mteHotOID (OID 1.3.6.1.2.1.88.2.1.4)	Set to the OID of the UCD table that contains the data that triggered the event.
mteHotValue (OID 1.3.6.1.2.1.88.2.1.5)	Set to 0 if the trap is not an error Set to non-zero if an error condition is being reported (generally 1).
mteFailedReason (OID 1.3.6.1.2.1.88.2.1.6)	Set to a string describing the reason the alert was sent.