CHAPTER 13

Using the Endpoint Console

This chapter includes the following topics:

Overview

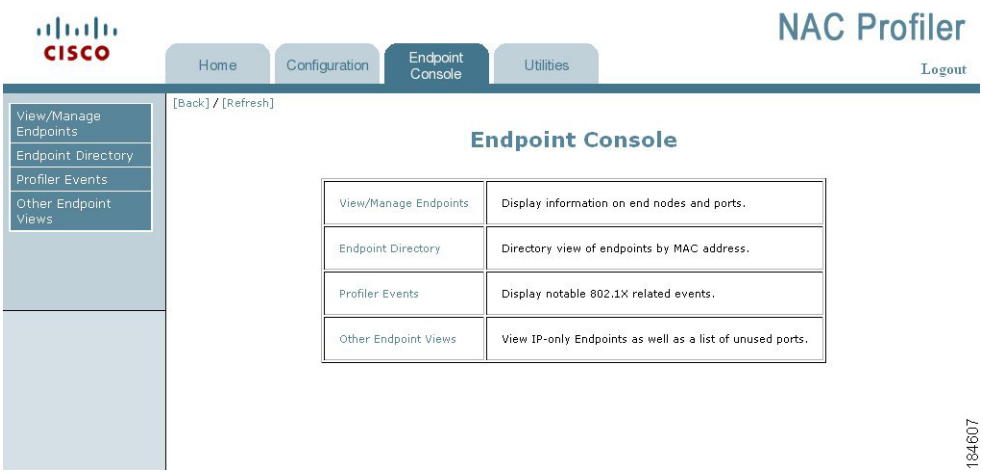
The NAC Profiler user interface provides the ability to view and manage the endpoints connecting to the enterprise network. The Endpoint Console tab of the User Interface provides several views of endpoint data that allow for the display of information about the endpoints, current and historical, as well as information regarding the connection status of all endpoints in the environment.

The different views provided in the Endpoint Console provide the primary user interface for monitoring the Endpoint Profiling and Behavior Monitoring functionality of NAC Profiler. Several options for viewing the current state of the Profiles and endpoints are provided for both the Directory and Port Provisioning modes of the system introduced earlier in this guide. The views themselves provide insight into the endpoint landscape, the effectiveness of the Profiles to classify all endpoints being observed on the network as well as providing the ability to drill-down into current and historical information collected by NAC Profiler on each endpoint. In addition, summary information regarding the Profiles enabled for population by NAC Profiler into the NAC Appliance system can be ascertained at a glance. Lastly, the Endpoint Console also provides the NAC Profiler interface for the display and management of Profiler Events which were described in Chapter 10, "Configuring NAC Profiler Events."

This chapter outlines the different endpoint and event views provided by the Endpoint Console.

Figure 13-1 shows the main Endpoint Console page that provides access to the endpoint and event views. All Endpoint Console functionality is initiated from this page, by selecting the link in the table, or selecting an option from the left-hand navigation pane.

Figure 13-1 Endpoint Console Main Page



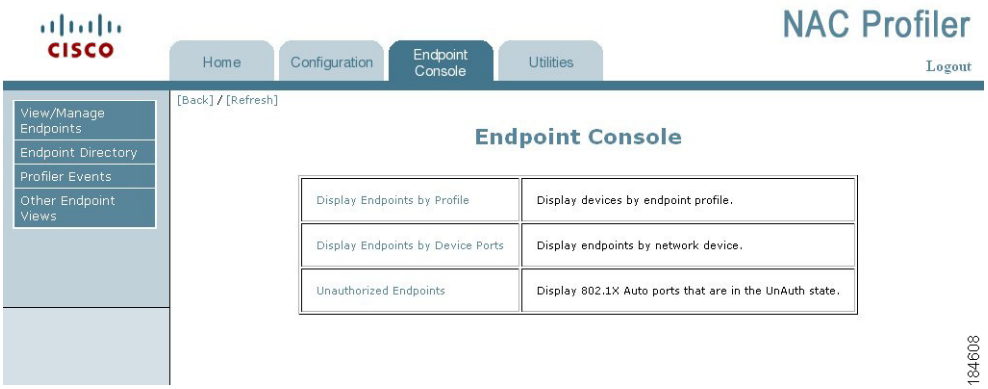
Viewing and Managing Endpoints

The Endpoint Console provides two primary methods for viewing the endpoints connected to the network, their current Profile and associated data: View/Manage Endpoints and the Endpoint Directory. View/Manage Endpoints provides several different options for viewing endpoint information and utilizing the Port Provisioning capability of Cisco NAC Profiler. The Endpoint Directory provides the views used in Directory deployments of NAC Profiler, providing views of endpoint information without the port management options used in port provisioning mode. The Endpoint Directory also provides summary information about the current configuration of integration of NAC Profiler with NAC Appliance and other authentication systems interacting with the NAC Profiler database via LDAP. The Other Endpoint Views section includes IP only endpoints and a list of ports to which nothing is attached.

View/Manage Endpoints

The first and most detailed view of endpoints and associated data is via the View/Manage Endpoints option selected from table of the Endpoint Console page which is displayed whenever the Endpoint Console tab is selected. Selecting View/Manage Endpoints displays the following table which provides several options for viewing endpoints and providing the Port Provisioning interface for making changes to NAC and 802.1X authentication related network device port settings such as Link State, VLAN, and 802.1X settings (e.g., Force-UnAuth, Auto, Force-Auth). Figure 13-2 shows the views that become available via the selection of View/Manage Endpoints from the main Endpoint Console page.

Figure 13-2 View/Manage Endpoints



Display Endpoints by Profile

As the title suggests, this view displays the Profiles that are currently enabled and any associated endpoints. Figure 13-3 shows the table of Profiles displayed in the interface when Display Endpoints by Profile is selected.

Figure 13-3 View Endpoints by Profile

[Back] / [Refresh]

Table of Profiles (Date last viewed: 07/9/2007 - 8:52 am)

Profiles	Total Assets	Connected Assets	Port Control
APC UPS	8	8	View Manage Set All
Apple Users	128	128	View Manage Set All
Hewlett-Packard JetDirect Printer	26	26	View Manage Set All
IP Phone	3	3	View Manage Set All
Linux Users	23	23	View Manage Set All
Mail Server	2	2	View Manage Set All
Multi Server	9	9	View Manage Set All
PXEClient	1	1	View Manage Set All
Sun User	2	2	View Manage Set All
Unknown	5	5	View Manage Set All
Windows 98 Users	3	3	View Manage Set All
Windows OS	2	1	View Manage Set All
Windows Users	285	285	View Manage Set All
XBox	3	3	View Manage Set All
Dell Network Printer	0	0	
LinkSys	0	0	
NetGear	0	0	
Sun OS	0	0	
Web Server	0	0	
Xerox Phaser Printer	0	0	
Unprofiled Ports	447		View Manage Set All

Total Assets: 500 Total Connected Devices: 499

184772

Immediately adjacent to the table heading is a date/time stamp of when the Table of Profiles was last viewed. Changes to the Total Assets and Connected Assets since the last view for each Profile are indicated by a “+” or “-“ value adjacent to the current value to reflect additions or removals from the total or connected endpoint counts.

The default sort order is by Profile name (ascending). Note the table can be sorted by Total Assets or Connected assets by selecting the column name. Selecting any of the column names toggles between an ascending and descending sort order of the table by the selected criteria.

The following is a description of each of the table columns:

- Profiles—a list of the Profiles that are currently enabled. Profiles that contain endpoints are listed first, the Profile name is a link to a drill-down table of endpoints in the Profile. If the profile name link is selected, the table of endpoints currently in the selected Profile is displayed, as shown in Figure 13-4.
- Total Assets—the total number endpoints that have been classified into this Profile.
- Connected Assets—the endpoints that have been classified into this Profile and that are currently connected to the network according to the most current information in the NAC Profiler database.
- Port Control—contains three buttons: View, Manage, and Set All. The View button displays the drill-down table of all endpoints currently in the selected profile along with summary information. This is the same table that is displayed if the profile name link is selected from the table as described above, and as illustrated in Figure 13-4.

Figure 13-4 Table of Endpoints

[Back] / [Refresh]

Table of APC UPS
Total Profiles: 8 Summary

MAC	IP Address	Certainty	Switch IP Port	Link	802.1X	VLAN
00:c0:b7:fd:a8:47 (AMERICAN POWER CONVERSION CORP)	10.11.20.157	96%	Hamilton East Gi4/47 (146)	Up	Force Auth (Auth)	Default (1)
00:c0:b7:67:fd:8f (AMERICAN POWER CONVERSION CORP)	10.12.20.17	96%	Hamilton West Gi4/47 (146)	Up	Force Auth (Auth)	Default (1)
00:c0:b7:06:0f:02 (AMERICAN POWER CONVERSION CORP)	10.13.20.124	96%	Hayes Gi4/47 (146)	Up	Force Auth (Auth)	Default (1)
00:c0:b7:88:72:72 (AMERICAN POWER CONVERSION CORP)	10.14.20.143	96%	Wilson Gi3/47 (98)	Up	Force Auth (Auth)	Default (1)
00:c0:b7:fd:21:f3 (AMERICAN POWER CONVERSION CORP)	10.15.20.10	96%	Roosevelt Gi1/0/23 (10123)	Up	Force Auth (Auth)	Default (1)
00:c0:b7:cd:c8:78 (AMERICAN POWER CONVERSION CORP)	10.15.20.155	96%	Roosevelt Gi2/0/23 (10623)	Up	Force Auth (Auth)	Default (1)
00:c0:b7:fc:ec:10 (AMERICAN POWER CONVERSION CORP)	10.15.20.167	96%	Roosevelt Gi3/0/23 (11123)	Up	Force Auth (Auth)	Default (1)
00:c0:b7:25:77:4d (AMERICAN POWER CONVERSION CORP)	10.15.33.15	96%	Lincoln Gi1/0/23 (10123)	Up	Force Auth (Auth)	Default (1)

184774

Mac Vendor Summary	Total
AMERICAN POWER CONVERSION CORP	8

The table of endpoints which is displayed when a Profile name link is selected, or the when the View button in the Port Control column for the Profile is selected has six columns that display the summary information from the database pertaining to each of the endpoints currently in the Profile.

- MAC—shows the MAC address of each endpoint. If the OUI of the MAC address resolves to a known MAC Vendor, the MAC Vendor is displayed in parentheses beneath the MAC in hexadecimal format. The MAC address is a link that will cause the MAC Endpoint Summary to be displayed in the UI. The MAC Endpoint Summary will be described in detail later in the chapter.
- IP Address—displays the current IP address of the endpoint if it is known. The IP address of the endpoint is a link that will display the IP Endpoint Summary of the endpoint if selected. The IP Summary Information page will be described later in the chapter.
- Certainty—displays the current Certainty value for the endpoint which is calculated based on the rule or rules in the Profile that currently test true.
- Switch IP Port—displays the current location of the endpoint if it is currently connected and known by NAC Profiler. The switch name (as entered in the Network Device configuration), IP address and the port identifier are displayed. The IFIndex number of the port is displayed in parentheses.
- Link—shows the status of the port link state as reported by the network device.

- 802.1X—shows the status of the port 802.1X authenticator. In parentheses below the setting the port state will show ‘Auth’ for endpoints that have successfully completed 802.1X authentication or auth has been forced, and ‘UnAuth’ for those that have failed or have been forced to UnAuth.
- VLAN—shows the current VLAN the port is operating in. If the network device was configured with VLAN name-to-VID mappings (see Chapter 8, “Adding Network Devices to the NAC Profiler Configuration”), the VLAN Name will be shown. If mappings were not included in the network device configuration, the VLAN column will show the VID the port is currently assigned to.

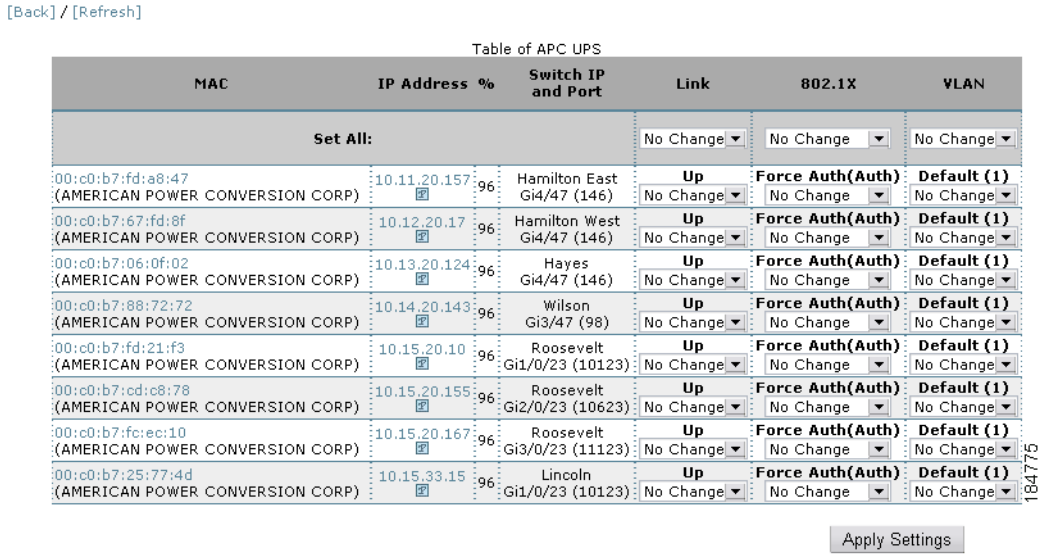
Using the Manage View

The Manage button brings up a different view of endpoints by profile. The Manage view is used primarily when employing NAC Profiler in the Port Provisioning mode. As shown in Figure 13-5, it displays similar information about all the endpoints in a selected Profile (e.g., using the View button or selecting the Profile name link), but in addition shows the current state of selected attributes: Link State, 802.1X and VLAN of the network device port providing network connectivity to each endpoint in the Profile. The Manage view also allows these selected parameters to be changed as will be discussed below.

Note NAC Profiler utilizes the SNMP protocol to make changes to selected parameters on the network devices in its database. In order to change any network device parameter using the Manage view or other views used for Port Provisioning mode, the network device configuration in NAC Profiler must have the Read-Write community string for each device.

Changes to network device configuration is made persistent on the network device through the use of the “Save Configuration” option in the network device configuration (see Chapter 8, “Adding Network Devices to the NAC Profiler Configuration”). If this option is checked for a device, and saving configuration changes made via SNMP is supported by the device manufacturer, changes made via NAC Profiler port provisioning will be persistent. See Figure 13-5.

Figure 13-5 View Endpoints by Profile: Manage View



In the Manage view, selecting an endpoint MAC or IP brings up the summary information for the MAC or IP respectively as described in the last section, and detailed later in the chapter.

Note the drop-down boxes beneath the current state of the Link, 802.1X and VLAN parameters for the port connecting each endpoint. In Port Provisioning mode, these drop-downs can be used to selectively change these three parameters on the edge network device providing connectivity for the selected endpoint or endpoints (typically access switches). The choices for each of the parameters are as follows:

- Link State—up, or administratively down. Changing the Link State to down on a port effectively places the port in an admin down state until it is returned manually to the up state.
- 802.1X—allows the following settings to be selected on the ports of network devices with 802.1X authentication implemented and enabled:
  - Auto – 802.1X authentication enabled
  - Force UnAuth – Port placed in unauthenticated state, administratively down
  - Force Auth – Port placed in authenticated state administratively, 802.1X authentication effectively disabled and the device is allowed to communicate without authenticating
- VLAN—allows the port to be administratively assigned to any VLAN name specified in the network device configuration (VLAN Name-to-VID mapping, see Chapter 8, “Adding Network Devices to the NAC Profiler Configuration”).

The very first row of the table serves a special purpose, and is referred to as the “Set All” row. This row can be used to set the parameters selected in the Link State, 802.1X and VLAN columns on all ports in the remaining rows of the table. This function can be used to set parameters on all ports under NAC Profiler management that are providing connectivity to the endpoints currently in the Profile. For example, it could be used to place all endpoints in a Profile for UPS devices into the network infrastructure VLAN. The desired VLAN would be selected from the drop-down menu for the VLAN parameter in the Set All row, and the Apply Settings button selected. This would result on any port with an endpoint in the selected Profile to have the VLAN setting changed to the selected VLAN name (VID).

The Apply Settings button at the bottom of the table is used to commit the changes. Upon selecting Apply Settings, Cisco NAC Profiler will execute the SNMP sets required to make the changes on the network devices affected by the change.

Using the Set All View

The Set All button brings up a special-purpose version of the Manage view of endpoints by profile, used exclusively in the Port Provisioning mode. It utilizes the same ‘Set All’ functionality described for the top row of the manage view, but does so without the need to view the ports or the associated endpoints that are to be configured. It is used exclusively for setting port parameters (link state, 802.1X state, and VLAN) on all ports providing connectivity to the devices currently in the selected Profile. Figure 13-6 shows the Set All view.

Figure 13-6 View Endpoints by Profile: Set All View

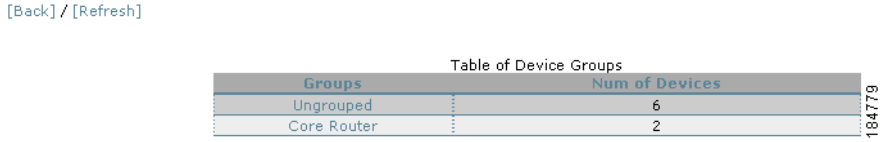
To use the Set All view, choose the value of the selected parameter(s)—Link, 802.1X and or VLAN—from the drop-down list and select the Apply Settings. NAC Profiler will change the selected port settings on all network devices that have endpoints in the profile connected to them via SNMP.

Display Endpoints by Device Port

An alternative way to view endpoints via the NAC Profiler interface is by displaying endpoints by network device port. This view provides a device-level view of what endpoints are connected along with their Profile on a port-by-port basis. Ports that do not have an endpoint connected are depicted as well as ports that are serving as trunks. As with the other views in the Endpoint Console, the view allows the user to drill-down into the MAC and IP Summary pages for each endpoint.

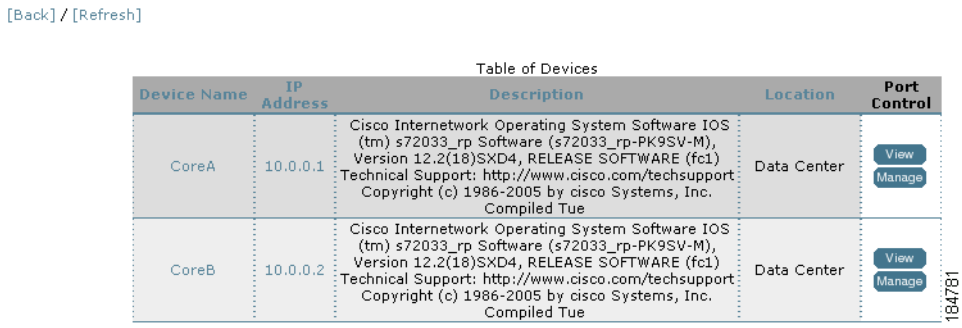
To display Endpoints by Device port, select that option from the Endpoint Console which will display the table of Device Groups as shown in Figure 13-7.

Figure 13-7 Table of Device Groups



Selecting the group name from this table will display the list of network devices in the selected device group. (If device groups are not being used, select the “Ungrouped” group name to display all network devices). Figure 13-8 shows the table of devices that would be displayed which allows selection of the specific network device to display endpoints by port on.

Figure 13-8 View Endpoints by Device



This table is similar to that displayed when listing network devices except that it includes a column called ‘Port Control’ which contains two buttons, View and Manage.

Selecting the View button, the Device Name or IP address of a network device brings up the view of the network device as shown in Figure 13-9.

Figure 13-9 View Endpoints by Device: Device-level View

[Back] / [Refresh]

Table of Hamilton East

Port	Profile	MAC	IP Address	Link State	802.1X	VLAN
Gi1/1 (2)	Trunk Port			Down	Force Auth (Auth)	Default (1)
Gi1/2 (3)	Trunk Port			Down	Force Auth (Auth)	Default (1)
Gi2/1 (4)	Apple Users	00:0d:93:09:3f:24 (Apple Computer)	192.168.20.138	Up	Force Auth (Auth)	Default (1)
Gi2/2 (5)	Windows Users	00:c0:4f:23:df:1a (DELL COMPUTER CORPORATION)	192.168.20.94	Up	Force Auth (Auth)	Default (1)
Gi2/3 (6)	Apple Users	00:14:51:6b:47:24 (Apple Computer Inc.)	192.168.20.25	Up	Force Auth (Auth)	Default (1)
Gi2/4 (7)	Apple Users	00:14:51:bc:ce:09 (Apple Computer Inc.)	192.168.20.165	Up	Force Auth (Auth)	Default (1)
Gi2/5 (8)	Apple Users	00:14:51:57:a4:6c (Apple Computer Inc.)	192.168.20.30	Up	Force Auth (Auth)	Default (1)
Gi2/6 (9)				Down	Force Auth (Auth)	Default (1)
Gi2/7 (10)	Windows Users	00:c0:4f:50:9a:06 (DELL COMPUTER CORPORATION)	192.168.20.56	Up	Force Auth (Auth)	Default (1)
Gi2/8 (11)	Windows Users	00:14:22:72:79:3a (Dell Inc.)	192.168.20.218	Up	Force Auth (Auth)	Default (1)
Gi2/9 (12)	Windows Users	00:06:5b:8c:2c:93 (Dell Computer Corp.)	192.168.20.48	Up	Force Auth (Auth)	Default (1)
Gi2/10 (13)	Apple Users	00:11:24:e5:f6:69 (Apple Computer)	192.168.20.120	Up	Force Auth (Auth)	Default (1)
Gi2/11 (14)	Linux Users	00:90:27:70:3d:5f (INTEL CORPORATION)	192.168.20.96	Up	Force Auth (Auth)	Default (1)
Gi2/12 (15)				Down	Force Auth (Auth)	Default (1)

184783

By default, this view displays each port on the device (by ascending port number/ifIndex) and the endpoint or endpoints connected to that port in the NAC Profiler database. It is possible for more than one endpoint connected to a single port. If for example there is a switch that is either unmanaged (such as the integrated switch in an IP Phone) or not entered in the NAC Profiler database or a Wireless Access Point or hub, multiple endpoints will be discovered and displayed as connected on a single port of a network device.

The table can be re-sorted by selecting the desired column heading. Select the desired column heading once for ascending order sort, twice for descending. The following describes each column of the table:

- Port—displays the network device port number. The value in parentheses is the ifIndex which provides a consistent reference to the port number on the device.
- Profile—for each endpoint in the database currently connected to the port, the current Profile for that endpoint will be displayed.
- MAC Address—for each endpoint in the database currently connected to the port, the MAC address of the endpoint will be displayed in hexadecimal format, with the MAC Vendor (if the OUI resolves to a vendor) displayed in parentheses below. The hexadecimal MAC address is a link. Selecting the link will direct the user interface to the MAC Endpoint Summary page which is described later in this chapter.
- IP Address—for each endpoint in the database currently connected to the port, if the NAC Profiler has current IP address information in the database for the endpoint the current IP host address of the endpoint is displayed. The endpoint IP host address is a link. Selecting the link will direct the user interface to the IP Endpoint Summary page which is described later in this chapter.

For ports that have been determined to be Trunks by NAC Profiler, the first three columns are replaced with a single entry ‘Trunk Port’ as shown on port Gi1/1(2) in Figure 13-9. No MAC, Profile or IP information is displayed on Trunk Ports.

- Link State—Reflects the current link state setting of the port. Down indicates that the port has been administratively disabled. Up indicates that the endpoint is active and connected to the network.

- 802.1X Setting and PAE State—no entry indicates 802.1X disabled (or not supported), Auto, ForceAuth or ForceUnAuth. Below the setting in parentheses the state of the PAE is indicated: Auth, or UnAuth.
- VLAN—indicates the VLAN name (if configured) or VID of the port.

The Manage View Option of View Endpoints by Device Port

Selecting the Manage button for a network device brings up a different view of endpoints by device port. The Manage view of endpoints by device port (Figure 13-10) is used primarily when employing NAC Profiler in the Port Provisioning mode. It displays similar information about all the endpoints connected to the selected network device on a port-by-port basis, and in addition shows the current state of selected attributes: Link State, 802.1X and VLAN of the network device port providing network connectivity to each endpoint. The Manage view also allows those selected parameters to be changed as discussed below.

Figure 13-10 View Endpoints by Device: Manage View

Table of archimedes-3750

Port	Profile	MAC	IP Address	Link State	802.1X	VLAN
Set All:				No Change	No Change	No Change
Gi1/0/1 (10101)				Up No Change	No Change	1 No Change
Gi1/0/2 (10102)				Up No Change	No Change	1 No Change
Gi1/0/3 (10103)				Down No Change	No Change	1 No Change
Gi1/0/4 (10104)		00:03:47:93:b6:d5 (Intel Corporation)		Up No Change	Force Auth(Auth) No Change	7 No Change
Gi1/0/5 (10105)	Unknown	00:03:47:93:b6:d6 (Intel Corporation)	10.1.1.1	Up No Change	Force Auth(Auth) No Change	5 No Change
Gi1/0/6 (10106)				Down No Change	No Change	1 No Change
Gi1/0/7 (10107)				Up No Change	No Change	1 No Change
Gi1/0/8 (10108)				Up No Change	No Change	1 No Change
Gi1/0/9 (10109)				Up No Change	Force Auth(Auth) No Change	5 No Change

184615

The primary difference with this view and the previous is the addition of the “Set All” row in the table, and the addition of the drop-down menus for the selected port parameters which are similar to the previously described Manage views.

The choices for each of the parameters provided in the dropdown menus are as follows:

- Link State—up, or administratively down. Changing the Link State to down on a port effectively places the port in an admin down state until it is returned manually to the up state.
- 802.1X—allows the following settings to be selected on the ports of network devices with 802.1X authentication implemented and enabled:
  - Auto—802.1X authentication enabled
  - Force UnAuth—Port placed in unauthenticated state, administratively down
  - Force Auth—Port placed in authenticated state administratively, 802.1X authentication effectively disabled
- VLAN—allows the port to be administratively assigned to any VLAN name specified in the network device configuration (VLAN Name-to-VID mapping, see Chapter 8, “Adding Network Devices to the NAC Profiler Configuration”).

The first row of the table serves a special purpose, and is referred to as the "Set All" row. This row can be used to set the parameters selected in the Link State, 802.1X and VLAN columns on all ports in the remaining rows of the table, which is effectively every port on the network device.

Unauthorized Endpoints

The Unauthorized Endpoints view is used exclusively in environments in which 802.1X port-based authentication has been deployed. The purpose of this view is to display all endpoints throughout the environment that are connected to ports in the UnAuth state. These endpoints are essentially disconnected from the 802.1X-enabled network due to failing to successfully complete authentication (e.g., do not have valid credentials or may not have a properly configured supplicant, etc.), or are on ports that are set to Force UnAuth. The view provides a way to quickly determine what endpoints are in this state, and where (by switch and port) which can, in turn, be utilized for providing support to these users/devices.

Endpoint Directory View

The Endpoint Directory is the primary view used in most deployments of NAC Profiler. The Endpoint Directory View displays all Profiles in the environment along with summary information about the Profile. Essentially the Endpoint Directory view is designed to provide a dashboard view into the Profiles, the endpoints in the Profiles, and how NAC Profiler is currently configured to interact with NAC Appliance and other authentication servers. It does not include the mechanisms necessary to interact with the network devices as in the Directory deployment model, such interaction is typically not necessary since the ongoing configuration and/or enforcement mechanisms commonly reside in the NAC system itself. Figure 13-11 shows the Endpoint Directory view.

Figure 13-11 Endpoint Directory

[Back] / [Refresh]

Table of Profiles in Directory

Profiles	Num of Matches	LDAP	CCA
APC UPS	8	No	UPS[30%]
Apple Users	128	No	-
Hewlett-Packard JetDirect Printer	26	No	Printers[30%]
IP Phone	3	No	IP Phones[30%]
Linux Users	23	No	-
Mail Server	2	No	-
Multi Server	9	No	-
PXEClient	1	No	-
Sun User	2	No	-
Unknown	5	No	-
Windows 98 Users	3	No	-
Windows OS	2	No	-
Windows Users	285	No	-
XBox	3	No	Games[30%]

Total Matches: 500

184786

Note that the Endpoint Directory view allows for filtering the table of Profiles. The Filter drop-down menu in the top right corner of the main pane allows the Endpoint Directory to be filtered by the network names specified in the My Networks configuration. If there are multiple networks in the My Networks configuration, the Endpoint Directory can be presented for all networks (show all), or alternatively for a single network name from the My Networks configuration by selecting the network name from the Filter drop-down.

The columns of the Table of Profiles are described below:

- Profiles—All Profiles in Cisco NAC Profiler that contain endpoints are displayed. The default sort of the table is by Profile Name (ascending), selecting the Profiles link selects the Profile Name as the sort field and alternating between ascending and descending sort order.

- Num of Matches—Displays the number of endpoints currently in the Profile. The table sort can be changed to this field by selecting the Num of Matches column heading.
- LDAP—Indicates whether the Profile is enabled for authentication via LDAP. In implementations where NAC Profiler will serve as an external database, Profiles that are enabled for LDAP will indicate so in this column. “Yes” indicates that NAC Profiler will respond to a MAC authentication request via LDAP for endpoints in the Profile.
- NAC—The NAC column indicates whether or not there is currently a NAC Event enabled that will match the Profile. A ‘-’ in the column indicates that there are no enabled NAC Events that match the Profile and can be interpreted as endpoints in that Profile will not be added to the Filter List on the CAM. If there is a NAC Event name in the column for a given Profile, the minimum certainty value for that NAC Event will also be reflected.

Each of the Profile names in the table is a link that will display a more detailed view into each Profile. Select the Profile name link to display the summary view of the selected Profile. See Figure 13-12.

Figure 13-12 Endpoint Directory: Profile View

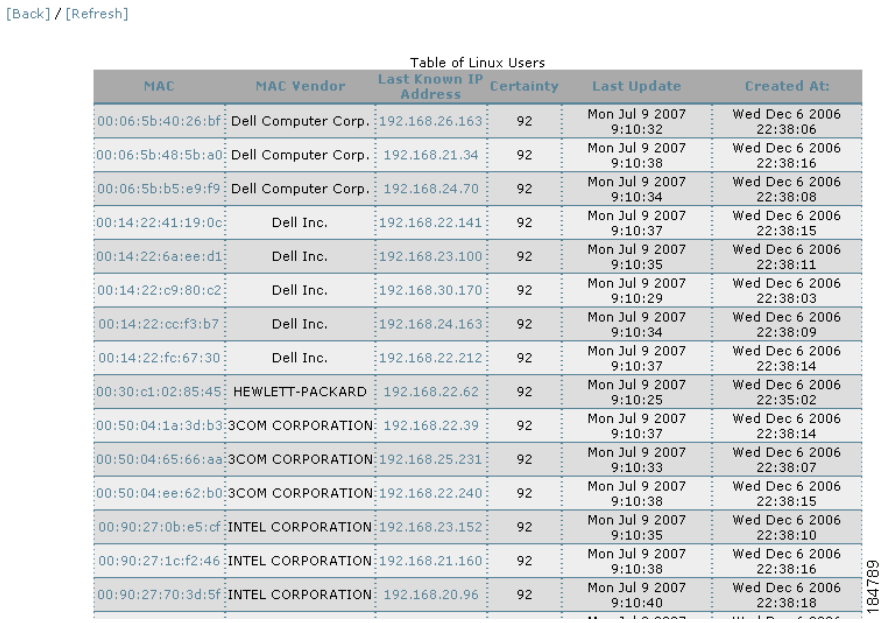

[Back] / [Refresh]

Table of Linux Users

MAC	MAC Vendor	Last Known IP Address	Certainty	Last Update	Created At:
00:06:5b:40:26:bf	Dell Computer Corp.	192.168.26.163	92	Mon Jul 9 2007 9:10:32	Wed Dec 6 2006 22:38:06
00:06:5b:48:5b:a0	Dell Computer Corp.	192.168.21.34	92	Mon Jul 9 2007 9:10:38	Wed Dec 6 2006 22:38:16
00:06:5b:b5:e9:f9	Dell Computer Corp.	192.168.24.70	92	Mon Jul 9 2007 9:10:34	Wed Dec 6 2006 22:38:08
00:14:22:41:19:0c	Dell Inc.	192.168.22.141	92	Mon Jul 9 2007 9:10:37	Wed Dec 6 2006 22:38:15
00:14:22:6a:ee:d1	Dell Inc.	192.168.23.100	92	Mon Jul 9 2007 9:10:35	Wed Dec 6 2006 22:38:11
00:14:22:c9:80:c2	Dell Inc.	192.168.30.170	92	Mon Jul 9 2007 9:10:29	Wed Dec 6 2006 22:38:03
00:14:22:cc:f3:b7	Dell Inc.	192.168.24.163	92	Mon Jul 9 2007 9:10:34	Wed Dec 6 2006 22:38:09
00:14:22:fc:67:30	Dell Inc.	192.168.22.212	92	Mon Jul 9 2007 9:10:37	Wed Dec 6 2006 22:38:14
00:30:c1:02:85:45	HEWLETT-PACKARD	192.168.22.62	92	Mon Jul 9 2007 9:10:25	Wed Dec 6 2006 22:35:02
00:50:04:1a:3d:b3	3COM CORPORATION	192.168.22.39	92	Mon Jul 9 2007 9:10:37	Wed Dec 6 2006 22:38:14
00:50:04:65:66:aa	3COM CORPORATION	192.168.25.231	92	Mon Jul 9 2007 9:10:33	Wed Dec 6 2006 22:38:07
00:50:04:ee:62:b0	3COM CORPORATION	192.168.22.240	92	Mon Jul 9 2007 9:10:38	Wed Dec 6 2006 22:38:15
00:90:27:0b:e5:cf	INTEL CORPORATION	192.168.23.152	92	Mon Jul 9 2007 9:10:35	Wed Dec 6 2006 22:38:10
00:90:27:1c:f2:46	INTEL CORPORATION	192.168.21.160	92	Mon Jul 9 2007 9:10:38	Wed Dec 6 2006 22:38:16
00:90:27:70:3d:5f	INTEL CORPORATION	192.168.20.96	92	Mon Jul 9 2007 9:10:40	Wed Dec 6 2006 22:38:18

184789

This view provides summary information about all endpoints currently in each Endpoint Profile in the Directory. The default sort order of the table is by MAC Address (first column) but the sort can be specified on any of the columns by selecting the column heading. Sort order can be toggled between ascending and descending by selecting the column heading.

The following is a description of each column of the table:

- MAC Address—Indicates the MAC address of each endpoint in the Profile in hexadecimal format. The MAC address of the endpoint is a link. Selecting the link will direct the user interface to the endpoint MAC Summary page which is described later in this chapter.
- MAC Vendor—The MAC vendor the OUI of the MAC address resolves to.
- Last Known IP Address—Indicates the last known IP address of the endpoint. The endpoint IP host address is a link. Selecting the link will direct the user interface to the IP Summary page which is described later in this chapter.

- Certainty—Indicates the Certainty value calculated based on the rule(s) in the Profile that were matched for the endpoint.
- Last Update—Timestamp of the last update to data about the endpoint processed by the NAC Profiler engine.
- Created At—Timestamp of when the endpoint was first added to the Profile.

MAC Endpoint Summary

The MAC Endpoint Summary provides very detailed current and historical information about each endpoint in the NAC Profiler Database. As has been outlined in the chapter, the MAC Endpoint Summary view of an endpoint can be displayed from all views in the Endpoint Console and throughout the user interface. Throughout the NAC Profiler UI, if a MAC address is presented as a link, selecting that link will take the user to this view of the endpoint.

As described in Chapter 11, "Integration with Cisco NAC Appliance", entries populated by NAC Profiler into the Filter List on the CAM have a link (hostname/IP of NAC Profiler) in the endpoint description. Clicking this link from the CAM displays the same endpoint MAC Endpoint Summary from within the NAC Appliance user interface.

Figure 13-13 shows the MAC Endpoint Summary for an endpoint.

Figure 13-13 MAC Endpoint Summary

The endpoint summary provides a snapshot of the most current information about the endpoint in summary form. The following is a description of each of the summary data points displayed about an endpoint on the Summary:

- MAC Vendor—The MAC Vendor the OUI of the MAC Address resolves to.
- Latest IP Address Mapping—Current IP host address for the endpoint is displayed if a mapping for the MAC is known by NAC Profiler.

Note If the IP address is not known (e.g., NAC Profiler not able to establish the current IP address of the device through available data), the message "Currently there is no IP/MAC mapping for [MAC address]" is displayed under the MAC Vendor and the View IP History option (described below) is unavailable for the endpoint.

- Current Location—Displays the switch by name (if configured), IP address and current port (name and ifIndex in parentheses) of the network device providing connectivity to the endpoint if it is known to NAC Profiler. If the endpoint is not connected, or the current location of the endpoint is not known, this part of the summary is not included in the summary view.

  When the current location is known, the port name/ifIndex displayed as the current location of the endpoint is a link. Selecting that link will open the View Endpoint by Device Port view, with the entry for the endpoint shown in the first row of the table.

- System Location—If the network device providing connectivity to the endpoint has the system location OID of the System MIB populated, system location will be displayed as well.

- Current Profile(s)—presents a table that shows the Profile (or Profiles) that the selected endpoint MAC address is currently matching in the NAC Profiler database. Recall that an endpoint can be in one and only one Profile at any given time. However, there are oNACsions when an endpoint may in fact match similar rules in more than one Profile. This table in this view shows the Profile or Profiles which the endpoint matches with the respective level of Certainty based on the rule or rules matched in each of the current Profiles.

Immediately below the Current Profiles, the Endpoint Summary will reflect the 802.1X capability of the endpoint, either that it is or is not 802.1X capable if it is currently Profiled.

The 802.1X capability of the endpoint is reflective of the "802.1X Enabled" setting in the configuration of the endpoint's Profile as outlined in Chapter 9, "Configuring Endpoint Profiles." Unprofiled or Unknown endpoints will not have any indication of 802.1X capability.

At the bottom of the Endpoint Summary, links to additional views of information about the selected endpoint are provided. These additional endpoint-specific views are described in detail below.

View Layer 2 Trace

This view presents a table that indicates the path traffic from the selected endpoint is being observed traversing through the layer 2 local network for that endpoint. By determining the network devices and ports the endpoint is learned on (through examination of the SAT(CAM) tables of the devices), NAC Profiler can "trace" how traffic from the endpoint moves from the edge (access port) to the core, or the nearest routed boundary, of the network.

View MAC History

This view presents all information about the MAC Address of the selected endpoint available in the NAC Profiler database over the historical period.

Note The length of the historical period is determined by the Server module parameter "Historical Limit." Historical Limit is the number of days into the past which endpoint data is maintained in the NAC Profiler database (see Chapter 6, "NAC Profiler Server Configuration"). The default value for this parameter is 30 days and defines the historical period for all NAC Profiler historical views.

The MAC history view of an endpoint consists of three tables:

- Table of MAC History by port – shows the port(s) that this endpoint has connected to over the historical period.

Note If the MAC has not been connected to other network device ports during the historical period (e.g., endpoint has not been moved), the table will have the entry "No MACs were found" will be displayed.

- Table of MAC History by IP – shows the IP addresses that NAC Profiler has resolved to this MAC address over the length of the historical period.
- Table of MAC History by Profile – shows the Profile(s) that the endpoint has been classified into over the length of the historical period.

View Profile Data

For each MAC Address that has been discovered by NAC Profiler, this view presents a view of selected Profiling-related data observed by NAC Profiler for the endpoint during the historical period.

The Profile Data view for a selected endpoint consists of three tables:

- Table of Software Data – user agents, server banners,
- Table of Traffic Data – examples are: data flows observed occurring to/from the endpoint network stack information, and open ports
- Table of Other Data – examples are: DHCP, and SNMP SysDescr.

View IP History

For endpoints that NAC Profiler has current IP information for, this view allows the examination of information about the IP address itself. Especially for host addresses that are in the pool of addresses assigned via DHCP, the endpoints using a particular address may change frequently. This view provides a summary of information about the IP address, what endpoints have used it and where within the historical period.

Note If NAC Profiler is not able to map an IP host address to the MAC address of the endpoint, the View IP History link will not be presented in the MAC Endpoint Summary for the endpoint.

The IP History view of a selected endpoint/host address consists of two tables:

- Table of History by MAC – shows each MAC address NAC Profiler has observed using the current IP host address of the endpoint during the historical period. The first entry in the table is always the MAC address of the selected endpoint.
- Table of History by Profile – shows the Profile(s) that endpoints using the IP Host address over the historical period have been classified into.

The MAC Endpoint Summary also has a link, Clear Endpoint. Clear endpoint is used to cause the data about an endpoint to be cleared from the database. The data that is cleared about an endpoint includes IP and all Profile data. The MAC address of the endpoint is maintained in the database however.

Clear Endpoint can be used to cause Cisco NAC Profiler to transition the endpoint back to an unknown state, forcing the system to re-learn what it can about the endpoint and re-Profiling it once data is relearned.

IP Endpoint Summary

Like the MAC Endpoint Summary, the IP Endpoint Summary provides very detailed current and historical information about the endpoints in the NAC Profiler Database but from the perspective of the current IP host address. As has been outlined in the chapter, the IP Endpoint Summary view of an endpoint can be displayed from all views in the Endpoint Console and throughout the user interface. Throughout the NAC Profiler UI, if an IP address is presented as a link, selecting that link will take the user to this view of the IP Endpoint Summary View.

The information presented in the Endpoint Summary resulting from selecting an IP host address link is identical to that described for the MAC version of the Endpoint Summary. Essentially the only difference is the selection of IP versus MAC Address.

In addition, the optional views available through the selection of the links at the bottom of the Endpoint Summary are the same for the IP Endpoint Summary as well.

Other Endpoint Views

In addition to the endpoint views already discussed in this document, there are two additional, special purpose endpoint views in the Endpoint Console. Selecting Other Views from the main Endpoint Console page or from the left-hand navigation menu provides the ability to select the remaining two endpoint views: IP Only Endpoints and Unconnected Ports.

IP Only Endpoints provides a view of endpoints for which NAC Profiler has only IP information. MAC and location information for these endpoints has yet to be discovered by the system. When IP Only Endpoints are viewed, they are organized by Profile, and a table similar to View Endpoints by Profile is presented, however, in the case of IP Only Endpoints, drilling down into a Profile containing IP only endpoints reveals a table with only two columns: the IP host address of the endpoint and the Certainty. Selecting an IP address of an IP only endpoint from this table will display the IP Endpoint Summary which will allow the Profile Data and IP History for the IP address to be viewed.

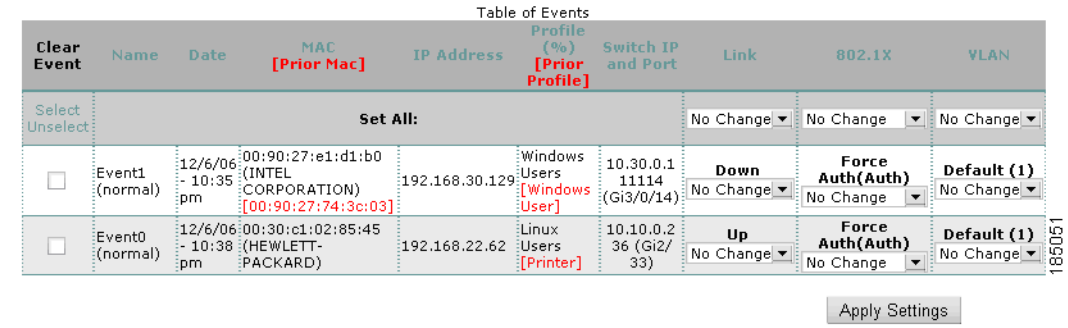
Unconnected Ports provides a list of all open ports on network devices in the configuration. By default network devices are listed by device name and IP Address in a table that shows the port name and ifIndex and media type of all available ports on each device.

Displaying and Managing Profiler Events from the Endpoint Console

The endpoint console also provides the interface within the NAC Profiler UI used for displaying and managing Profiler Events that are designated to be displayed in the Profiler interface in the event configuration. The configuration of Profiler Events was detailed in Chapter 10, “Configuring NAC Profiler Events.” The NAC Profiler interface is but one of the options available for the display of Newly Profiled, Profile Change and MAC Change Events detected by the system. In this section, the use of the Endpoint Console for displaying, interpreting and managing Profiler Events is outlined. Note that NAC events are not displayed in this interface; the results of the NAC events can be seen in the Endpoint Directory by analyzing the NAC column and the associated endpoints.

To view/manage Profiler events from the Endpoint Console, select Profiler Events from the table on the main page or from the left-hand navigation menu (Figure 13-14).

Figure 13-14 Table of Profiler Events



The Table of Events is the primary interface for viewing and managing Profiler Events that have been configured within the event configuration for the Profile Interface to be among the selected event delivery methods. All Newly Profiled, Profile and MAC change events that occur will be recorded in this interface and will remain in the table until manually cleared as described below.

For each event recorded by Cisco NAC Profiler, detailed information about the event is provided. In addition, the Profiler event interface allows for changes to be made to selected network device port parameters if Cisco NAC Profiler has locating (e.g., switch and port number providing connectivity to the endpoint) information about the endpoint generating the event. In addition, the "set all" row is displayed allowing changes to be made to multiple ports (e.g., all ports providing connectivity to the endpoints generating events currently displayed in the table) simultaneously as described in the Endpoint event views earlier in the chapter.

The follow describes the data in each column of the table for the three event types:

- Clear Event—The checkbox in each of the rows of the table is used to select the event for clearing in combination with the Apply Settings button at the bottom of the table.
- Event Name—For each event in the table, this column will reflect the name of the Event (from event configuration) resulting in the table entry. Immediately below the name, the event severity as configured in the event is also displayed in parentheses.
- Date—Reflects the date and time the Profiler event occurred.
- MAC/[Prior MAC]—Displays the MAC address and MAC Vendor of the endpoint triggering the event. In the case of MAC Change Events, the MAC Address of the endpoint connected to the port last is displayed under the current MAC in brackets.
- IP Address—Displays the IP address of the endpoint triggering the event if known by Cisco NAC Profiler.
- Profile/[Prior Profile]—Displays the Profile of the endpoint triggering the event. In the case of Profile Change Events, the Profile that the endpoint was in immediately previous to the change is displayed as the Prior Profile.
- Switch IP and Port—Displays the current location (e.g., switch and port providing connectivity) of the endpoint triggering the event if known by the NAC Profiler. Format is Switch IP, Interface name, and ifIndex. If the current location of the endpoint is not known, 0.0.0.0 and 0 will be displayed in this column, and current port settings for Link, 802.1X and VLAN as described below will be unpopulated.

Beyond the switch IP and Port are the current values of selected parameters of the port connecting the endpoint triggering the event. Note that drop down menus are provided for each parameter that are used in conjunction with the Apply Changes button to changed selected parameters of ports. Above the drop down menu, the current state of the port is reflected for each of the parameters as follows:

- Link State—Reflects the current link state setting of the port. Down indicates that the port has been administratively disabled. Up indicates that the endpoint is active and connected to the network.
- 802.1X Setting and PAE State—no entry indicates 802.1X disabled (or not supported), Auto, ForceAuth or ForceUnAuth. Below the setting in parentheses the state of the PAE is indicated: Auth, or UnAuth.
- VLAN—indicates the VLAN name (if configured) or VID of the port.

  The choices for setting each of the port parameters provided by the drop-down menus are as follows:

  – Link State—up, or administratively down. Changing the Link State to down on a port effectively places the port in an admin down state until it is returned manually to the up state.

  – 802.1X – allows the following settings to be selected on the ports of network devices with 802.1X authentication implemented and enabled:

    - Auto—802.1X authentication enabled

    - Force UnAuth—Port placed in unauthenticated state, administratively down

    - Force Auth—Port placed in authenticated state administratively, 802.1X authentication effectively disabled

  – VLAN—allows the port to be administratively assigned to any VLAN name specified in the network device configuration (VLAN Name-to-VID mapping, see Chapter 8, “Adding Network Devices to the NAC Profiler Configuration”).

If the Events interface is used to make changes to port parameters, use the Apply Changes button to execute changes. In order for network device parameters to be changed via this interface, NAC Profiler must have read-write SNMP access to the device or devices being re-configured.

Clearing Profiler Events

Profiler Events displayed in the Endpoint Console will remain in the table of events for the length of the historical period if not manually cleared.

To manually clear events, select the Clear Event checkbox of the event or events that should be cleared from the first column of the table of events. Selecting the Apply Changes button with event(s) selected for clearing will result in the event(s) being permanently cleared from the table and the database.