



CHAPTER 9

Configuring Endpoint Profiles

This chapter contains the following topics:

- [Overview, page 9-1](#)
- [Saving a New Rule to an Endpoint Profile, page 9-8](#)
- [IP Address Rule, page 9-8](#)
- [Traffic Rules, page 9-9](#)
- [Application Rule, page 9-13](#)

Overview

NAC Profiler uses its network analysis function to examine network attached endpoint traffic and classify it according to pre-determined behavior patterns. By matching traffic types to known endpoint profiles, NAC Profiler can make several inferences about who or what is attached to each network access port. Of most importance in this process is the determination of whether the endpoint represents a network resource, a user of network resources or a combination of both. This determination has implications in the deployment of authentication, IT security and network admission control (NAC).

Using NAC Profiler, administrators have the ability to define the types of information they wish to monitor, classify and manage. NAC Profiler contains a set of options used to create rules based on the hardware addresses, network protocol addresses or applications being carried in data packets. Combined with NAC Profiler's network mapping capability, it is possible to know exactly what kind of device or user is attached to each port and make determinations about whether the endpoint(s) should be provisioned to NAC Appliance. Additionally, the understanding of the location and type of these endpoints can also be used as a system for making configuration changes to the switch ports to which endpoints are attached.

Understanding Endpoint Profile Certainty

NAC Profiler performs the Endpoint Profiling function by aggregating identifying attributes of an endpoint and its behavior to ascertain the device's type. The accuracy of endpoint profiling performed by NAC Profiler is reflected in a measure of Certainty or confidence level that the device is currently in the correct profile. Each rule when created/added to an Endpoint Profile is assigned an individual certainty value which is reflective of how well the rule testing true predicts that the device belongs to the Profile the rule is bound to.

A device graduates into only one Profile at any given time based on one or more rules that have tested to be true based on observation by the NAC Profiler Endpoint Profiler system. The Certainty values are not hard-coded because the relative certainty for different kinds of behavior will vary from one enterprise network to the next. In general the rules added to a profile should be architected so that the more compelling aspects of an endpoint's behavior cause the Certainty value to increase more than less compelling attributes of the machine or its behavior. This ensures that the identity of the device will be driven more by the unique characteristics of its own type as opposed to attributes that might be shared with other device types.

For instance, the MAC address of an endpoint is often useful as a starting point in identifying the endpoint type, however, this value is easily copied ("spoofed") by someone wanting to gain unauthorized network access. As a result, a best-practice in constructing the rules utilized in Endpoint Profiles is to assign lower certainty values for the MAC vendor rule, while providing higher certainties to rules of other rule types such as protocol behavior, OS behavior, or DHCP vendor class. These identifiable aspects of endpoint behavior are inherently more complex, and hence more unlikely to be utilized in attempts to gain unauthorized network access, and therefore are more likely to result in an accurate Endpoint Profiling of end stations of that type.

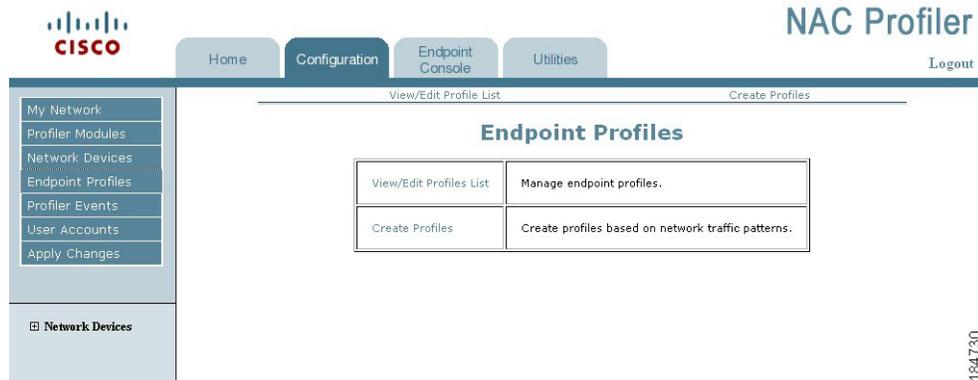
Enabling Existing Endpoint Profiles

The NAC Profiler Endpoint Profiler ships with a number of predefined Endpoint Profiles that have been created and tested in field deployments. These Profiles can be re-used as-is if desired, or may be modified as the situation dictates. In addition, they serve as templates for creating new profiles as outlined later in this section, and illustrate how different rule types and varying levels of certainty can be used to accurately Profile devices.

To view the list of Endpoint Profiles that are currently available in the system configuration, navigate to the Configuration tab, and select Endpoint Profiles option from the global navigation menu in the far left hand pane, or select Endpoint Profiles from the leftmost column of the table on the main Configuration page. Select View/Edit Profile List to display the Endpoint Profiles currently saved in the system configuration.

Creating New Endpoint Profiles in Cisco NAC Profiler Configuration

Profiles are created by selecting the Create Profiles link from the Endpoint Profiles table displayed in the Profiles Configuration Page as shown in [Figure 9-1](#).

Figure 9-1 Endpoint Profiles Configuration Page

Upon selecting the Create Profiles link, the Add Profile page displays containing the Add Profile form illustrated below.

Figure 9-2 Add Profile Form

Complete the following portions of the form to begin creation of a new Endpoint Profile.

Profile Name

Enter a unique name to help identify what endpoints this Profile will contain, such as Windows Web Users or HP Printers.

Description

Enter a brief description for this device. A common use of this field is to document the rules that it contains. This information will be displayed in the Table of Profiles in the column labeled Description. The Table of Profiles can be selected at any time to view summary information about the Endpoint Profiles currently configured.

802.1X enabled

Select the appropriate radio button to specify whether devices matching this profile are enabled for 802.1X authentication. Set to 'no' by default.

This option is an informational attribute applied to the endpoints contained within the Profile. NAC Profiler does not use this value for any configurations.

Profile enabled

Select the appropriate radio button to specify whether this profile is to be enabled or disabled. The default is enabled which will activate the Profile immediately upon the next Apply Changes -> Update Modules.

Allow timeout

This Profile attribute determines whether the Profile being created will be subject to the timeouts specified in the Server configuration as described in [Chapter 6, “NAC Profiler Server Configuration.”](#) Specifically, this is used to enable the Endpoint and Directory Timeouts on a profile-by-profile basis. The default is “no” meaning that even if an Endpoint or Directory timeout value is specified in the Server configuration, Profiles that do not have this attribute enabled will not be subjected to endpoint or directory timeout.



Note If an Aging Interval and Penalty are specified in the Server configuration, the interval and penalty are applied to all Profiles globally. This cannot be specified on a profile-by-profile basis.

When finished entering the parameters in Add Profile form, select the Add Profile button to save the new Endpoint Profile to Cisco NAC Profiler configuration. At this point the new Profile is added to the configuration but there are no rules bound to the Profile and endpoints will not be added to the Profile by the NAC Profiler Modeler. Rules must be added to the Profile as described in the paragraphs below.

Upon selecting the Add Profile button, a new page displays in the browser that includes the Save Profile form, illustrated below. This form shows the data captured in the first step of the Profile creation process outlined above, and allows for one or more rules to be added to the Profile via the buttons under the Add Rule heading in the form. Adding rules to the Profile enables Cisco NAC Profiler to begin classifying endpoints to the Profile assuming it is enabled, and an Apply Changes -> Update Modules is performed after saving the Profile with the rules. A button is provided for each available rule type that is used in the construction of Profiles.

To add a rule or rules to a Profile, select the button for the desired rule type to display the rule creation page(s) for the selected rule type.

Figure 9-3 Save Profile Form

The screenshot shows the 'Save Profile' form with the following elements:

- Profile Name:** [Text input field]
- Description:** [Text input field]
- 802.1x enabled:** Yes No
- Profile enabled:** Yes No
- Allow timeout:** Yes No
- LDAP:** Yes No
- Rules:** None Configured
- Add Rule:**
 - MAC Address
 - IP Address
 - Traffic
 - TCP Open Port
 - Application
 - Advanced
- Bottom Buttons:** Set Static, Save Profile, Delete Profile

NAC Profiler Rule Types

The NAC Profiler rules provide several ways in which to classify endpoints with specific attributes into an Endpoint Profile. The option of adding multiple rules of multiple rule types to a given Profile is supported. The rules used in constructing Endpoint Profiles can utilize a number of different criteria that range from layer 2 to layer 7 information that can be gleaned by the NAC Profiler Collectors from endpoint traffic or other sources of information to be outlined in this chapter. The available NAC Profiler Rule types are as follows:

- **MAC Address**—NAC Profiler maintains a list of all OUI values for MAC address vendor assignments. MAC Vendor rules allow the endpoints MAC address to be used as a criteria for classification into a Profile.
- **IP Address**—NAC Profiler can use the host address of endpoints to classify devices using host IP addresses within a designated range as a criterion for classification into a Profile.
- **Traffic**—Analysis of traffic information at layers 3-4. Based on information gathered by either the NetWatch collector module (traffic analysis) or NetRelay collector module (Netflow data exported from a Netflow-capable device).
- **TCP Open Port**—Layer 4 port information that is gathered either by monitoring SYN-ACK information passively or via the Active Profiling capabilities of NetInquiry described later in this chapter.
- **Application**—Analysis of application layer behavior including DHCP, Server Banners, DNS names, User Agents, etc.
- **Advanced**—Used to create complex expressions using AND, OR, and/or NOT, or to aggregate multiple rule logic into a single rule.

When multiple rules are configured for a profile, each is assigned a Certainty value. It is important to understand that traffic matching both rules will never produce a combined certainty in excess of 100%. For example, two 80% certainty rules being matched will not yield a 160% certainty or even a 100% certainty. The result will be much higher than 80% (96%, to be exact in this case), but not equal to or greater than 100%. Additionally it is important to understand that endpoints do not need to match ALL rules in order to be classified by NAC Profiler into a given Profile. When multiple rules are included in a Profile, NAC Profiler utilizes the logical OR operation, which results in endpoints being classified into the Profile when any one rule is satisfied. To create a combination of rules with Boolean logic other than 'OR' please refer to the Advanced Rule section of this document.

The following sections of the Configuration Guide outline the process for creation of rules within Profiles. Rule creation is an extremely important aspect of NAC Profiler configuration for Endpoint Profiling and Behavior Monitoring. To conceptualize the relationship between Profiles and Rules, the reader should think of NAC Profiler Profiles as logical containers which endpoints with similar characteristics and capabilities are sorted into via the Endpoint Profiling process. Rules are specified for each Profile and they are utilized by Cisco NAC Profiler to determine the criteria or logic by which the endpoints on a network should be classified (assigned) into a Profile.

The rules contained or bound to a profile provide the logic that Cisco NAC Profiler will use in making the Endpoint Profiling decision that is the decision to place an endpoint in a Profile, or in some cases moving an endpoint from one Profile to another based on the latest available information.

As will be illustrated in this section, NAC Profiler itself provides the administrator with information that can be utilized in the construction of rules. NAC Profiler maintains a database of information that the collector modules have gathered in the environment. For example, all of the MAC Vendor Names in packets observed by NAC Profiler are recorded in the system and can be viewed in the course of construction of new MAC Vendor rules based on the observation that devices using that MAC Vendor string are active on the network.

The following sections outline each of the NAC Profiler rule types and instructions for the configuration of these rules as they are added to Endpoint Profiles.

MAC Vendor Rule

A MAC Vendor rule enables Endpoint Profiling decisions based on information gleaned from the MAC address of the device. NAC Profiler can discover the MAC addresses of stations on the network via a number of mechanisms. The most commonly used mechanism for gathering MAC information is the regular query of edge network devices via SNMP. NAC Profiler examines the first three bytes (24 bits) of the MAC address (known as the Organizationally Unique Identifier, or OUI) of each MAC discovered by the system to determine the manufacturer of the device. When Cisco NAC Profiler is configured with a Profile containing a MAC Vendor Rule, endpoints observed using a MAC Address with the specified MAC Vendor String will be placed in the Profile based on the MAC Vendor Rule, at the assigned level of Certainty.



Note

When writing MAC rules, be aware that many vendors manufacture network interfaces used in a variety of endpoints; therefore, it may not be possible to identify the exact type of device using the MAC address alone.

In the Save Profile dialog box, click the MAC Vendor button. The Add MAC Vendor Rule page containing the Add MAC Vendor rule form displays on the page (Figure 9-4).

Figure 9-4 Add MAC Address Rule Form

Enter the following information in the form to create a MAC Vendor rule for a Profile:

MAC Vendor String

Enter the name of the vendor this Rule should match for classification into the Profile the Rule is being added to. To determine what MAC Vendor Strings NAC Profiler has observed in network traffic to date on 'Unknown' (un-profiled) endpoints, click the Show Data button. A pop-up which shows the MAC Vendor strings of endpoints currently in the Unknown profile is displayed on the interface as shown in Figure 9-5. Selecting the Show MAC/IP link following each MAC Vendor string in the table will display a list of the unknown endpoints with a MAC address resolving to that string by full MAC address (hexadecimal format) and IP address.

Figure 9-5 Show Data: Table of MAC Vendors

| MAC Vendors | Count |
|--|-------|
| Intel Corporation [Show MAC/IP] | 11 |
| Enterasys [Show MAC/IP] | 5 |
| Global Data Services [Show MAC/IP] | 4 |
| Hewlett Packard [Show MAC/IP] | 4 |
| Enterasys Networks [Show MAC/IP] | 3 |
| IBM Corporation [Show MAC/IP] | 3 |
| Allied Telesyn Inc. [Show MAC/IP] | 2 |
| Cisco Systems [Show MAC/IP] | 2 |
| 3 Com Corporation [Show MAC/IP] | 1 |
| Ambit Microsystems Corporation [Show MAC/IP] | 1 |
| ARCOM CONTROL SYSTEMS, LTD. [Show MAC/IP] | 1 |
| CANON INC. [Show MAC/IP] | 1 |

The MAC Vendor string field accepts a regular expression to match multiple forms of a MAC Vendor string. For example, Linksys devices have multiple OUIs registered with the IEEE that resolve to several different MAC Vendor strings including:

- The Linksys Group, Inc.
- Cisco-Linksys
- Cisco-Linksys, LLC
- Cisco-Linksys LLC



Note

A regular expression of `/linksys/i` entered in the MAC address String field matches all MAC Vendor strings including the string 'linksys' regardless of case. See [Application Rule, page 9-13](#) for more information about regular expressions.

Certainty

Enter a 'Certainty' value to apply to this rule. This is the relative measure of Certainty that an Endpoint profiled by this rule has been profiled accurately as outlined earlier in this chapter.

When finished defining the MAC vendor rule, select the Add MAC Vendor Rule button at the bottom of the Add MAC Vendor Rule form to save the changes, adding the newly created MAC Vendor Rule to the Profile.

Saving a New Rule to an Endpoint Profile

As previously described in [MAC Vendor Rule, page 9-6](#), upon successfully saving a new Rule to a Profile, the Save Profile page for the Profile being configured with a new rule displays in the browser. Note that the rule added in the previous steps is now displayed in the Save Profile form along with all other Profile attributes including previously configured rules as shown in [Figure 9-6](#).

Figure 9-6 Save Profile Form Showing a MAC Address Rule

The screenshot shows the 'Save Profile' form with the following details:

- Profile Name:** APC UPS
- Description:** Based on DHCP Vendor and/or M
- 802.1x enabled:** Yes No
- Profile enabled:** Yes No
- Allow timeout:** Yes No
- LDAP:** Yes No
- Rules List:**
 - App: /^APC\$/ (DHCP Client Vendor) [90%]
 - MAC: /^AMERICAN POWER CONVERSION CORP\$/ [60%]
- Buttons:** Edit, Remove, Add Rule (with sub-buttons: MACAddress, IP Address, Traffic, TCP Open Port, Application, Advanced), Set Static, Save Profile, Delete Profile.

Endpoint Profiles may contain one or more rules as required. As a new rule is added to a Profile, the Save Profile form appears. Any of the existing attributes of the Profile may be edited from the Save Profile form as described later in this chapter. New rules of any of the NAC Profiler Rule types may be added to the Profile using the procedures outlined in this chapter, beginning with the selection of the appropriate button for the rule type to be added.

When all desired rules have been added to the Profile, selecting the Save Profile button at the bottom of the form will save all changes to the Profiles and its associated rules to Cisco NAC Profiler configuration. In order for the new Profile to become part of the running configuration however the Profile must indicate 'enabled' in the Table of Profiles and an Apply Changes -> Update Modules performed. Upon the system restart the Profile will become active, and any endpoints in the NAC Profiler Endpoint database that match the rules specified in the new Profile will move from the Unknown profile into the new Profile, or from other enabled Profiles subject to the Certainty rules outlined earlier in the chapter. In order for endpoints to transition from an existing Profile other than Unknown into the new Profile, the Certainty value of the matching rule or rules in the new Profile must be higher than the current Profile.

IP Address Rule

An IP Address rule enables Endpoint Profiling decisions based on information gleaned from the IP header of the traffic originated by endpoints. NAC Profiler examines the Source IP address of network traffic to find matches with IP Address Rules. Endpoints observed using a host address specified within an IP Address Rule will be placed in the Profile containing the IP Address Rule, at the assigned level of Certainty.

This rule type is useful when all endpoints of a device-type of interest on a given network are assigned host addresses on a specific IP subnet. For example, if all 10.10.x.x addresses are assigned to printers, an IP Address Rule can be a very effective Rule to add to a Profile that is created to contain all the printers on the network.

To add an IP Address Rule to a selected Profile, from the Save Profile page for the selected Profile, click the IP Address button. The Add Address Rule page containing the form illustrated below will display in the browser.

Figure 9-7 Add Address Rule Form (IP Address Rule)

Enter the following information in the form to create an IP Address rule for inclusion in a Profile:

IP Address

Enter the IP address hosts should be using in order to match the rule and be moved into the Profile containing the IP Address rule. From the earlier example if the devices desired to be placed in this Profile were all assigned a host address on the .10 subnet of the 10.0.0.0 Class A network, 10.10.0.0 would be entered in this field.

Mask

Enter the subnet mask that should be applied to the specified IP Address. For example, to match all hosts on the .10 subnet of the 10.0.0.0 Class A network, a mask of 255.255.0.0 would be entered so that all hosts assigned on address on this subnet would match the rule.

Certainty

Enter a 'Certainty' value to apply to this rule. This is the relative measure of Certainty that an Endpoint profiled by this rule has been profiled accurately as outlined earlier in this chapter.

When finished, select the Add IP Address Rule button at the bottom of the Add IP Address Rule form to save the changes, adding the IP Address Rule to the Profile.

Upon successfully saving the Rule to the Profile, the Save Profile page for the Profile being configured will be displayed in the browser. Note that the IP Address Rule added in the previous steps will now be displayed in the Save Profile form with all other Profile attributes. At this point further edits/adds may be made to the Endpoint Profile, or the Profile changes may be saved.

Traffic Rules

A Traffic rule enables Endpoint Profiling decisions based on the observation by NAC Profiler of traffic flows having the characteristics specified in the rule:

- On a specific source or destination TCP or UDP port number
- From a specific source or to a specific destination IP, or to/from any IP.

Traffic rules contained within Profiles can greatly increase the certainty with which Endpoints are classified into that Profile, as this data is an easily distinguishable indicator of the services a device is providing or consuming on the network. Accordingly, they are often a highly reliable indicator of device type.

For example, to construct a Traffic Rule for Profiling printers proceed as follows: The Rule is constructed such that it examines network traffic for communication from the Print Server (IP Address of the rule is that of the Print Sever, with Source IP selected) to endpoints using the well-known destination port number of 9100. Traffic observed that matches this rule indicates the print server is communicating directly with a device for the purpose of printing. The device that the traffic is destined for is very likely to be a printer.

To add a Traffic Rule to a selected Profile, from the Save Profile page for the selected Profile, click the Traffic button. The Add Address Rule page containing the form illustrated below will display in the browser.

Figure 9-8 Add Traffic Rule Form

The screenshot shows a web form titled "Add Traffic Rule". It contains the following elements:

- A text input field for "IP Address (0.0.0.0 for any address):".
- Two radio buttons: "Source IP" (unselected) and "Destination IP" (selected).
- A text input field for "Source Port:" with the value "0".
- A text input field for "Destination Port:" with the value "0".
- A text input field for "Certainty:" followed by a "%" symbol.
- A button labeled "Add Traffic Rule".
- A vertical ID number "184737" on the right side of the form.

Enter the following information in the form to create a Traffic rule for inclusion in a Profile:

IP Address

Enter the IP Address to match and select Source IP or Destination IP to specify the direction of the communication. Note, other than 0.0.0.0, which is used to specify any address, this value must be a host address and not a subnet.

Source Port

Enter the Source Port that is expected in the communication. If this rule is looking at the Destination port, then enter 0 here.

Destination Port

Enter the Destination Port that is expected in the communication. If this rule is looking at the Source port, then enter 0 here.

Certainty

Enter a 'Certainty' value to apply to this rule. This is the relative measure of Certainty that an Endpoint profiled by this rule has been profiled accurately as outlined earlier in this chapter.



Note

When constructing Traffic Rules, the direction of the rule logic is important to consider. Use the following rule of thumb for determining the direction of traffic rules:

If the Source IP address is specified in the Traffic Rule (as in the printer example above), information about the **destination** IP address in the network traffic specified is gathered.

If a Destination IP address is specified in the traffic rule (example to follow), information about the **source** IP address in the network traffic specified is gathered.

For example: Web users are known to communicate with a web server on port 8080. A traffic rule could be utilized in the profile for web user, specifying the Destination IP in the rule to be the Web server's IP, with a destination port of 8080. This rule would be used for making a characterization about endpoints sourcing packets meeting this criterion—that endpoints observed transmitting packets satisfying this rule are highly likely to be running a web browser.

When finished, select the Add Traffic Rule button at the bottom of the Add Traffic Rule form to save the changes, adding the Traffic Rule to the Profile.

Upon successfully saving the Rule to the Profile, the Save Profile page for the Profile being configured will display in the browser. Note that the Traffic Rule added in the previous steps will now be displayed in the Save Profile form with all other Profile attributes. At this point further edits/adds may be made to the Endpoint Profile, or the Profile changes may be saved.

NAC Profiler Rules and NetInquiry

The NetInquiry module was introduced earlier in this Configuration Guide. NetInquiry is the NAC Profiler module that provides a means within Cisco NAC Profiler to actively probe an endpoint in order to generate a response from that endpoint that is useful in Endpoint Profiling. Essentially NetInquiry works by inducing endpoints of interest to initiate network conversations in a way that can be directly observed by Cisco NAC Profiler that allow those endpoints to be Profiled accurately. NetInquiry can be used to initiate communications from a specified set of endpoints in a way that is not harmful to endpoints or the network while aiding in the NAC Profiler endpoint profiling function.

Like the other NAC Profiler modules NetInquiry relies upon rules to define how it will operate in a given environment. The NAC Profiler rule types that are pertinent to NetInquiry are as follows:

- TCP Open Port rules
- The following Application rule types: Web Server Type, SMTP Server Banner, and DNS Name.

These rule types define how both NetWatch and NetInquiry operate in NAC Profiler system. Whether or not the optional NetInquiry functionality is used by Cisco NAC Profiler is controlled via a configuration option in each rule of the types that may be made to be active. (Assuming that is, that a NetInquiry module has been added to the configuration and is running on the system.) Recall that the NetInquiry modules in Cisco NAC Profiler run on the NAC Profiler Collector(s) deployed in the system. If one or more Collectors have had their NetInquiry module(s) configured and Profiles containing active rules are enabled, Cisco NAC Profiler will utilize Active Profiling techniques in addition to the passive techniques outlined throughout this chapter.

In the Add and Edit interface for the rule types with an Active capability listed above, the interface includes a configuration option, selected through a checkbox labeled 'Active.' The NetInquiry module(s) deployed in Cisco NAC Profiler will periodically initiate communications with the endpoints as specified in the NetInquiry module configuration for each Collector in the system configuration. This process repeats at the frequency specified in the NAC Profiler Server module configuration, according to Frequency parameter in the Active Profiling Configuration section of the NAC Profiler Server configuration. All NetInquiry modules in the system will initiate Active Profiling according to their respective configuration(s) at the specified frequency.

The configuration will result in required network traffic being generated by endpoints of interest and subsequently analyzed by Cisco NAC Profiler allowing the endpoints to be profiled quickly and accurately, particularly in cases where this traffic would be otherwise unavailable to NAC Profiler.

Additional information pertinent to the proper configuration of rules used by NetInquiry is provided in the following sections on configuring TCP Open Port and Application rules.

TCP Open Port Rule

A TCP Open Port rule enables Endpoint Profiling decisions based on NAC Profiler observing endpoints accepting TCP connections from other endpoints on TCP ports specified in the TCP Open Port rule.

This rule can be useful when endpoints accepting TCP communications on a known port indicates device type. For example, Compaq Insight Manager is known to use TCP port 2301 to communicate with servers running the Compaq Insight Manager Agent. When traffic is observed by NAC Profiler that indicates a particular endpoint has established a TCP connection on port 2301, it is a highly reliable indicator that the device that accepted the connection is running the Agent and is likely a server being managed by Insight Manager.

In the Save Profile dialog box, click the TCP Open Port button. The Add Port Rule dialog will display.

Figure 9-9 Add TCP Port Rule Form

The screenshot shows a web form titled "Add Port Rule". It contains the following elements:

- A text input field labeled "TCP Port:" followed by a "Show Data" button.
- A text input field labeled "Certainty:" followed by a percentage sign "%".
- A checkbox labeled "Active:".
- An "Add Port Rule" button at the bottom center.

The form is enclosed in a light gray border. A vertical label "184738" is visible on the right side of the form.

Enter the following information in the form to create a TCP Open Port rule for inclusion in a Profile:

TCP Port

Enter the TCP Port number to specify the TCP connection of interest for this rule. To see what TCP connections have been accepted by the endpoints yet to be profiled, click the Show Data button. To peruse all endpoint data, for endpoints that have been profiled and those that have not as yet, select the Profile Data option under the Utilities Tab from any page of the NAC Profiler web user interface.

Certainty

Enter a 'Certainty' value to apply to this rule. This is the relative measure of Certainty that an Endpoint profiled by this rule has been profiled accurately as outlined earlier in this chapter.

Active

Selecting this option enables the NetInquiry module functionality outlined in the last section of this chapter. When this option is selected, and a NetInquiry module is configured and running on one or more of the NAC Profiler collectors in the system, NAC Profiler will attempt to open a TCP session with the stations specified in the NetInquiry configuration.

When finished, select the Add Port Rule button at the bottom of the Add Port Rule form to save the changes, adding the Port Rule to the Profile.

Upon successfully saving the Rule to the Profile, the Save Profile page for the Profile being configured will display in the browser. Note that the TCP Open Port Rule added in the previous steps will now be displayed in the Save Profile form with all other Profile attributes. At this point further edits/adds may be made to the Endpoint Profile, or the Profile changes may be saved.

Application Rule

Application rules enable Endpoint Profiling decisions based upon the NAC Profiler observing network traffic containing application data that indicates device type. Application rules are in fact a family of rules that use observable attributes of several different types of endpoint traffic at the application layer to make inferences about the endpoint using its network traffic. In addition, the DNS Name type of application rules can make use of data held in the name service on the network in order to determine information about endpoints.

In the Save Profile form for a selected Profile, click the Application button. The Add Application Rule form will display allowing the creation of a new Application rule.

Figure 9-10 Add Application Rule Form

A drop-down menu in the 'Application Type' field allows you to choose one of the available Application rule types. The application rule types that can be used in the creation of an Application Rule are shown in Figure 9-11.

Figure 9-11 Add Application Rule—Selecting Rule Type

A description of the different Application rule types is provided below. (An asterisk after the rule type name designates that the application rule type can be used in conjunction with NetInquiry and Active Profiling as described earlier in this chapter.)

- **Web Server Type*** —Examines the traffic from web servers on the network responding to client requests to determine that the responding endpoint is a web server, along with its type (e.g., Apache or Microsoft IIS, for example).

When used optionally as an Active rule, NAC Profiler will attempt to initiate an HTTP session with the device(s) specified in the configurations of the NetInquiry module(s) running throughout Cisco NAC Profiler. Responses are analyzed for any web servers that respond to determine that the responding device is a web server along with the type of web server that establishes an HTTP session.

- **Web User Agent**—Examines traffic from endpoints to web servers, specifically client's requests to a web server and searches the User-Agent string in these requests. The User Agent string can be used to determine attributes of the endpoint that sent the traffic. For example, that the machine is running the Microsoft Internet Explorer on Windows.

- **Web URL**—Examines available HTTP traffic from endpoints to look for specific URLs. An example would be examining HTTP traffic to identify which endpoints are communicating with an anti-virus vendor's automatic updates site to identify devices likely to be Windows PCs.
- **SMTP Server Banner***—Examines protocol header information in endpoint traffic to identify e-mail traffic, and gleans the email server(s) address and type(s) passively from e-mail traffic.

When used optionally as an Active rule, SMTP Server Banner rules will result in the NAC Profiler communicating with hosts on address ranges specified in the configuration of the NetInquiry modules. Communication with existing SMTP servers in the range(s) will generate the traffic necessary to identify those servers and delivering it to the interface of the Collector where it can be analyzed.

- **DHCP Client Name**—Examines the payload of DHCP requests to determine the hostname of the client to find matches with specified text strings. This rule is helpful if the hostname indicates the end node type. For example, a hostname beginning with the prefix of 'BSTXP' could be known to be a Windows XP machine, while a hostname prefix of BSTPS is known to be a printer, DHCP Client Name rules could be utilized to Profile Windows machines and printers in this environment using data gleaned from DHCP traffic.
- **DHCP Client Vendor**—Examines the payload of endpoint DHCP requests to determine if identifying information about the vendor of the DHCP client stack is present. Many vendors will include information in this portion of the DHCP that identifies the device type making the request. For example Cisco 7960G IP Phones include the string 'Cisco Systems, Inc. IP Phone CP-7960G' in the DHCP Client Vendor portion of DHCP requests sent by these devices. Examining DHCP requests from endpoints and finding requests from endpoints containing this string is a high probability indicator that the device sending the request is a Cisco IP Phone.
- **DNS Name***—Examines DNS query/reply traffic on the network (forward and reverse lookups) for the purpose of discovering an endpoint's DNS name, thereby making it possible to match against endpoints with DNS names that contain specified strings. Similar to DHCP Client Name rules, DNS Name Rules can be utilized to identify endpoints by using DNS transactions observed on the network.

When used optionally as an Active rule, NAC Profiler will perform a reverse lookup on the host addresses specified in the NetInquiry modules in the system, gathering the DNS name of each host from the name server specified in the Server configuration.

- **SNMP System Description**—Examines SNMP traffic between network infrastructure (typically) and uses the sysDescr value as a criterion to identify infrastructure devices of a particular type.

It should be noted that Application Rules in their passive mode of operation will require that endpoint traffic to-from web servers, SMTP servers, the DHCP service or DNS resolvers on the network must be delivered to a monitoring interface on one or more of the Collectors running in Cisco NAC Profiler. Traffic redirection through SPAN or RSPAN is one method to redirect traffic of interest from the VLANs/subnets these services reside on to the monitoring interface on the CAS/Collector. In the Active mode, Cisco NAC Profiler communicates with the endpoints directly as described above in order to generate traffic at the management interface of the CAS/Collector so that it can be analyzed by NetWatch. The active method does not require redirection of native endpoint traffic to the monitoring interface of the Collector. Essentially in active mode, the Collector is inducing the endpoints in the specified range to send directed traffic of interest to the management interface of the Collector where it can be analyzed by NAC Profiler. The decision to employ passive versus active techniques is dependent on the specifics of each network environment. There are trade-offs associated with both methods, and full consideration should be given to devising a Profiling strategy that best meets the objectives of each implementation.

Once the Application Rule Type has been chosen, the next step in adding an Application Rule is to provide the specific parameters of the rule as dictated by the type.

For all types, the Application Rules specify a text string to be searched for in the packets delivered for analysis by either passive or active methods as described above. In the Search Data field of the

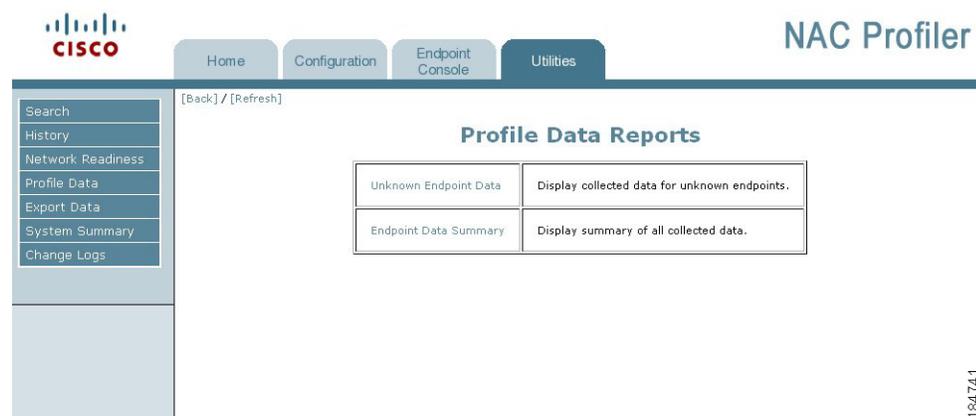
Search Data

As described above, the Application Rule types operate on the basis of examining application layer information in the network traffic of endpoints looking for specific contents in a designated area of the packet specific to the selected Application rule type. An example used previously is the DHCP Client Vendor rule that can be used to identify Cisco IP Phones, by matching the string ‘Cisco Systems, Inc. IP Phone CP-7960G’.

The Search Data portion of the Add Application Rule form is used for specifying the string that NAC Profiler will look for to identify endpoints that match the criteria. NAC Profiler employs Regular Expressions for specifying the search data for Application rules. A Regular Expression is a string that is used to describe or match a set of strings, according to certain syntax rules. Regular Expressions provide an extremely powerful and highly flexible method of specifying patterns to match. Before creating the Regular Expression however, it is good practice to first determine the string pattern or patterns that should be searched for using a Regular Expression.

Cisco NAC Profiler collects the data that the modules on the Collectors are observing, and makes the data available to the system administrator for the purposes of determining the available search data to use for constructing rules of the various types outlined in this chapter. This data is available by navigating to the Utilities tab and then selecting the Profile Data menu option which brings up the Profile Data Reports page in the interface, illustrated in [Figure 9-12](#).

Figure 9-12 Profile Data Reports Page



Selecting the Endpoint Data Summary link from the table takes the interface to the Endpoint Data Reports page. The reports accessible from this page show all endpoint information observed and catalogued by Cisco NAC Profiler, organized into the following categories:

- **Endpoint User Agents**—Displays Web Client User Agents for endpoints observed by NAC Profiler.
- **Endpoint Server Banners**—Displays Web and SMTP banners from endpoints observed by NAC Profiler.
- **Endpoint DHCP Vendors**—Displays DHCP Client Vendor strings from endpoint DHCP requests observed by NAC Profiler.
- **Endpoint Open Ports**—Displays endpoints observed by NAC Profiler to have specific open ports.

- **MAC Vendors**—Displays the MAC vendor strings (converted from IEEE registered OUIs observed by NAC Profiler on the network).
- **DNS Names**—Display DNS Names gathered by NAC Profiler as outlined in the description of the DNS Name application rule type earlier in the chapter.
- **SNMP Data**—Display sysDescr contents of SNMP traffic observed by NAC Profiler.

An example of one of the reports, Endpoint Server Banners, from a functional system is shown in Figure 9-13.

Figure 9-13 Endpoint Server Banners Example Report

| Table of Web Servers | |
|--|-------|
| Web Servers | Count |
| Apache [Show IPs] | 6 |
| cisco-IOS [Show IPs] | 3 |
| 3Com/v1.0 [Show IPs] | 2 |
| Allegra-Software-RomPager/4.20 [Show IPs] | 1 |
| Apache/2.2.0 (Fedora) [Show IPs] | 1 |
| Lanswitch - v100R003 HttpServer 1.1 [Show IPs] | 1 |
| YAWS/0.0.1 [Show IPs] | 1 |

| Table of SMTP Servers | |
|-----------------------|-------|
| SMTP Servers | Count |
| No SMTP Servers found | 0 |

The report shows the Web Servers and SMTP Servers from which NAC Profiler has observed traffic, and a count of the servers of each type. The first column of the table provides the string that is the identifier for the type of Web Server as observed by NAC Profiler in network traffic, and the string that would be used to create the Regular Expression as the Search Data in a Web Server Type application rule. This rule would be added to a Profile that would contain the endpoints running an Apache web server. That Web Server Type application rule would appear as shown in Figure 9-14.

Figure 9-14 Example of a Regular Expression in an Application Rule

Save Application Rule

Application Type: Web Server Type

Search Data: ^Apache

Certainty: 65%

Active:

Save Application Rule

Note the contents of the Search Data field of the Web Server Type application rule above. It contains the regular expression ^Apache.

The ^ in a regular expression is an “anchor character” in regular expressions that specifies start of a string. This regular expression will match any web server type then that begins with the string ‘Apache.’ Note that regular expressions are case-sensitive unless the pattern modifier ‘i’ is used to match the string regardless of case.

Some other example regular expressions include the following:

- The regular expression /Apple|Mac|CFNet/ will match any string containing the word ‘Apple’ or ‘MAC’ or ‘CFNet’ (case sensitive).

This regular expression was designed to be used in a Web User Agent rule in a Profile designed to contain apple users via observing their web traffic.

- `/^Dell Network Printer$/` will match only strings that begin with 'Dell' and end with 'Printer'

This regular expression would be used in a DHCP Client Vendor rule to Profile Dell printers into a Profile via observing this string in their DHCP requests.

- `/Windows\Win32/i` will match any string containing the word 'windows' or 'win32' regardless of case.

Similar to the first regular expression, this could be used in a Web User Agent rule to identify devices running Windows operating systems and Internet Explorer.

The preconfigured Profiles that are included in the NAC Profiler contain many examples of regular expressions used in a variety of Endpoint Profile rules. For more information and documentation on Regular Expressions, please see the following web references:

<http://www.regular-expressions.info/>

<http://www.cs.tut.fi/~jkorpela/perl/regexp.html>

<http://www.ilovejackdaniels.com/cheat-sheets/regular-expressions-cheat-sheet/>

After the Search Data for the Application Rule is entered complete the remaining parameters for the Application Rule being created/edited.

Certainty

Enter a 'Certainty' value to apply to this rule. This is the relative measure of Certainty that an Endpoint profiled by this rule has been profiled accurately as outlined earlier in this chapter.

When finished, select the Save Application Rule button at the bottom of the Add Application Rule form to save the changes, adding the IP Address Rule to the Profile.

Upon successfully saving the Application rule to the Profile, the Save Profile page for the Profile being configured will be displayed in the browser. Note that the Application rule added in the previous steps will now be displayed in the Save Profile form with all other Profile attributes. At this point further edits/adds may be made to the Endpoint Profile, or the Profile changes may be saved.

Active

This parameter is an option and will appear in the Add Application rule form for the following Application Rule types only: Web Server Type, SMTP Server Banner, and DNS Name. As outlined earlier in this section, selecting Active in Application Rules of these types enables the NetInquiry module functionality to actively probe/query the endpoints specified in the NetInquiry configuration for Web Server Type, SMTP server or DNS Name according to the rule Application Type.

Advanced Rules

The Advanced rule option offers the ability to define custom rules using Extensible Markup Language (XML) to combine the NAC Profiler rule types with Boolean logic operators as well as define pattern matches for any endpoint data observed and collected from endpoint traffic analyzed by NAC Profiler. For example, an Advanced Rule can be defined that looks at both the MAC Vendor String and DHCP options in DHCP requests from endpoints, applying the logical AND to both rules (meaning both have to test true in order for the rule to be satisfied). If both the MAC Vendor String and the DHCP options requested match what is specified in an Advanced Rule, the endpoint is likely to be of a particular type.

An advanced rule of this type can be designed to identify MAC OS devices that are using DHCP for addressing. Apple MAC OS DHCP requests contain a null DHCP Client Vendor, which makes the standard DHCP Client Vendor rule not useful for the Profiling of these devices. In a scenario where the Internet traffic from Apple users is not available for direct analysis by NAC Profiler such that a Web User Agent rule could not be used, if the MAC OS device utilized DHCP, the analysis of their DHCP requests by NAC Profiler might provide fruitful in Profiling the MAC OS endpoints.

To create a MAC OS Profile containing a single Advanced Rule that checks for the both the desired MAC Vendor String and a specified list of DHCP options, the following steps would need to be performed:

1. Create a new Profile from the Configuration tab, and name it Mac OS (it is imperative that the name match the name specified in the XML rule on line 2)
2. For the description, “Devices running Mac OS” should suffice
3. Select the Enable radio button and leave the others at default, select ADD PROFILE
4. This will bring up the Save Profile form for the newly created Mac OS profile with the ADD RULES section of the form enabled. Select the Advanced button to add an Advanced rule to this Profile. [Figure 9-15](#) shows the Add Advanced Rule form displayed.

Figure 9-15 Add Advanced Rule Form

5. The large text box next to the heading XML rule is used to enter the rule in XML format. Note that in the case of advanced rules, all parameters including the certainty value is contained in the XML text. In the example the Certainty for this rule is 75%.

The rule text in XML format is typically “cut & pasted” into the text box from an editor such as Windows Notepad, formatted and verified before committing to the rule. In our example the following text would be entered into the XML rule text box:

```
<Rule name="MacOSAdv">
  <RuleEntity entity="Mac OS" cf="0.75"/>
  <AND>
    <Vendor vendor="/^Apple/i"/>
    <DHCPReqOptions option-list="/^1,3,6,15,112,113,78,79,95"/>
  </AND>
</Rule>
```

6. The two rules this Advanced Rule consist of include a MAC Vendor Rule and a specific set of DHCP options included by the endpoint when it requests addressing information via DHCP. The MAC Vendor rule uses a regular expression to match any MAC Vendor strings beginning with the word ‘Apple’ regardless of case. Similarly, the DHCP options request must begin with the string indicated for a match to occur. The two <AND> statements indicate the beginning and end of the rules that are AND’ed together. In this case both rules must be true for this Advanced Rule to hold true.

When finished, select the Add Advanced Rule button at the bottom of the Add Advanced Rule form to save the changes, adding the Advanced to the Profile.

Upon successfully saving the Application rule to the Profile, the Save Profile page for the Profile being configured will be displayed in the browser. Note that the Application rule added in the previous steps will now be displayed in the Save Profile form with all other Profile attributes. At this point further edits/adds may be made to the Endpoint Profile, or the Profile changes may be saved.

Set Static

Beyond the six rule types outlined thus far in the chapter, the NAC Profiler has one additional means of classifying endpoints into an Endpoint Profile. The Set Static button at the bottom of the Save Profile form provides a way of designating specific endpoints by MAC or IP Address into an Endpoint Profile, at a specified level of certainty.

Selecting the Set Static button for a Profile brings up the form in [Figure 9-16](#) which allows for listing IP host addresses and or MAC addresses of endpoints to be placed in the Profile statically.

Figure 9-16 Set Static Profile Rule

When finished, select the Add Advanced Rule button at the bottom of the Add Advanced Rule form to save the changes, adding the Advanced to the Profile.

Upon successfully saving the Application rule to the Profile, the Save Profile page for the Profile being configured will be displayed in the browser. Note that the Application rule added in the previous steps will now be displayed in the Save Profile form with all other Profile attributes. At this point further edits/adds may be made to the Endpoint Profile, or the Profile changes may be saved.

To enter MAC addresses in the form, use the standard format 01:02:03:04:05:06, one MAC address per line. Enter IP host addresses in dotted decimal notation (e.g., 192.168.1.1), one per line.

Specify a Certainty value for devices added to the Profile via the Static Rule. Note that the Certainty mechanism continues to operate as previously described. If NAC Profiler observes behavior from an endpoint currently in a Profile via a static assignment that matches a rule or rules in another enabled

Profile, if the Certainty value of the new Profile is higher, the endpoint will transition Profiles. To ensure that endpoints assigned statically to a Profile never transition out of the Profile, be sure to assign a high certainty value to the static rule such as 100%.

Selecting the Save Static button will save the static assignments to the Profile and the interface will return to the Save Profile form for that Profile.

Editing Static Rule Sets in Profiles

Profiles containing static rule sets will have the following line in the rules section of the Save Profile form:

‘Static Rule Set (use button to modify)’

Unlike the other rule types which use the edit and remove radio buttons to edit/delete the rule, static rules require the use of the Set Static button, which will open the Static Addresses Form. Edit the addresses as required, or delete all addresses to remove the static rule set from the Profile.

View/Edit Profiles List

To view or edit the list of user- and system-created profiles select the View/Edit Profiles List option. [Figure 9-17](#) illustrates the View/Edit Profiles page that displays in the user interface listing all Endpoint Profiles currently saved to the system configuration.

Figure 9-17 View/Edit Profile List: Table of Profiles

The screenshot shows the NAC Profiler interface with the 'View/Edit Profile List' page. The table of profiles is as follows:

| Name | Description | 802.1x Aware | Enabled |
|-----------------------------------|--------------------------------------|--------------|---------|
| 3Com Gear | based on SNMP | No | Yes |
| Apache Server | Based on server banners | No | No |
| APC UPS | Based on DHCP Vendor and/or MAC | No | Yes |
| Apple Users | Based on User Agent | Yes | Yes |
| Apple Web Server | Based on User Agent | Yes | No |
| Cisco AP | Based on DHCP Vendor | No | No |
| Cisco AP c1200 | Based on DHCP Vendor | No | No |
| Cisco IP Phone (CP-7940G) | Based on DHCP Vendor | No | No |
| Cisco IP Phone (CP-7960G) | Based on DHCP Vendor | No | No |
| Cisco IP Phone (CP-7970G) | Based on DHCP Vendor | No | No |
| CO Testing | Telnet to bohr.research | No | No |
| Dell Network Printer | Based on DHCP Vendor | No | Yes |
| D-Link | Based on MAC Vendor | No | Yes |
| Etherboot | Based on DHCP Vendor | No | No |
| Hewlett-Packard JetDirect Printer | Based on DHCP Vendor and/or OpenPort | No | Yes |
| IIS Server | Based on server banners | No | No |
| IP Phone | Based on DHCP Vendor | No | Yes |
| Lab Laptop | ACS Test | No | Yes |
| LinkSys | Based on DHCP Vendor | No | Yes |
| Linux OS (2.4.x) | Based on DHCP | No | No |
| Linux OS (2.6.x) | Based on DHCP | No | No |
| Linux Router | SysInfo | No | Yes |
| Linux Users | Based on User Agent | Yes | Yes |
| Linux Users (2.4.x) | Based on User Agent | Yes | No |
| Linux Users (2.6.x) | Based on User Agent | Yes | No |
| Mail Server | Based on server banners | No | Yes |
| Multi Server | Based on server banners | No | Yes |
| NetGear | Based on DHCP Vendor | No | Yes |
| Polycom Phones | MAC Vendor | No | Yes |
| PXEClient | Based on DHCP Vendor | No | Yes |
| Sun OS | Based on DHCP Vendor Class | No | Yes |

For each Endpoint Profile in the Table of Profiles, summary information about the Profile is provided. The '802.1X Aware' column indicates whether or not the 802.1X radio button for the Profile is currently set to yes or no. Again, this is an entirely informational attribute that can be used to indicate whether or not the devices in a given Profile should have an 802.1X supplicant. The right-most column indicates whether or not the Profile is currently enabled.

Clicking any of the green hyperlink Profile Names in the leftmost column of the table will launch the Save Profile form for the selected Profile which will reflect the current configuration of the Profile illustrated below. This form allows the editing of any parameter of the Profile, including adding, editing or deleting rules from the Profile.

Figure 9-18 Profile Edit Dialog

The screenshot shows the 'Save Profile' dialog box for a profile named 'APC UPS'. The description is 'Based on DHCP Vendor and/or M'. The '802.1x enabled' radio button is set to 'No'. The 'Profile enabled' radio button is set to 'Yes'. The 'Allow timeout' radio button is set to 'No'. The 'LDAP' radio button is set to 'No'. There are two rules listed: 'App: /^APC\$/ (DHCP Client Vendor) [90%]' and 'MAC: /^AMERICAN POWER CONVERSION CORP\$/ [60%]'. Each rule has a radio button and a checkbox. Below the rules are 'Edit' and 'Remove' buttons. At the bottom, there are buttons for 'Set Static', 'Save Profile', and 'Delete Profile'. There is also an 'Add Rule' section with buttons for 'MACAddress', 'IP Address', 'Traffic', 'TCP Open Port', 'Application', and 'Advanced'. A vertical number '184735' is visible on the right side of the dialog box.

Editing Rules Previously Saved to a Profile

Selecting the Edit radio button to the immediate right of the Rule, and then clicking on the Edit button beneath the radio button(s) will bring up the Save Rule form for that rule. Use the directions outlined earlier in this chapter for changing rule parameters. Select the Save button at the bottom of the form to save the changes.

To remove a rule from an Endpoint Profiler, select the check box above the Remove button on the Save Profile form, then select the Remove button. The rule will be removed from the Profile permanently.

As mentioned in the section on Set Static, static rules must be edited/removed by selecting the Set Static button at the bottom of the Save Profile form, Make changes as required or remove all static entries and Save the static rule to commit the change.

