CHAPTER 6

Cisco NAC Profiler Server Configuration

This chapter contains the following topics:

- Overview, page 6-1
- Cisco NAC Profiler Server Configuration, page 6-2
- Server Network Connection Options on Cisco NAC Profiler Systems, page 6-3
  - Add Network Connection to Profiler Server Configuration of Type 'Server', page 6-5
  - Add Network Connection to Profiler Server Configuration of Type 'Client', page 6-6
- Editing Other Server Configuration Parameters, page 6-9
  - Database Maintenance, page 6-9
  - Network Mapping Configuration, page 6-12
  - Active Profiling Configuration/Profiling Configuration, page 6-14
  - External Reference, page 6-16
- Saving Edits to the Cisco NAC Profiler Server Configuration, page 6-17
- Editing a Profiler Server Network Connection Previously Added to the Configuration, page 6-17
- Removing a Profiler Server Network Connection, page 6-18

Overview

The next task associated with configuration of Cisco NAC Profiler is configuration of the Profiler Server. Recall that the web-based management interface is served by the Cisco NAC Profiler Server and it provides management of all components of the NAC Profiler system including modules running on the Collectors after establishment of network communications between the Profiler Server and the Collectors. Correct configuration of the Profiler Server at the outset ensures that the initial system configuration can be created and the system brought into service via the NAC Profiler UI.

When the Profiler Server and Collector(s) are initialized as described in Chapter 4, “Installation and Initial Configuration” a very basic system configuration is created, including initial configuration for the Profiler Server itself and the Forwarder modules on the Collectors across the system. The basic server configuration includes default parameters that allow the system to come up and be managed via the web interface so that further configuration can be completed via the UI to enable the Profiler Server for network communications with the Collectors, and begin endpoint discovery, profiling and identity monitoring in the target environment.

The Collector modules are initialized with the parameters required to communicate with the Server over the network in order to get their completed configuration and send endpoint data back to the Server for processing. Once the Profiler Server is configured successfully as described in this chapter, communication with the Collectors will be established so that collected endpoint data can be forwarded to the Server for processing into the database and the Collectors can get their full configuration from the Profiler Server. As communication with the Profiler Server is established by each Collector, a complete Collector configuration is completed as described in Chapter 7, "Configuring Collector Modules". Upon the execution of an Apply Changes -> Update Modules the NAC Profiler Server will create and send to each Collector its most current configuration then restarting the Collector so that the configuration on the Collector matches that shown in the UI.

Tip Prior to beginning the configuration of the NAC Profiler Server module as outlined in this chapter, the Collectors should have been started up and configured in accordance with the procedures outlined in Chapter 4, "Installation and Initial Configuration". The Collector Service on each NAC Profiler Collector should have been verified to be running using the CLI commands outlined in that chapter.

Cisco NAC Profiler Server Configuration

The configuration of the NAC Profiler Server is viewed and edited through a single page of the UI, which consists of a single form entitled Configure Server.

Navigation to the Configure Server form is provided directly from the Home Tab, which is the default start page for all new sessions to the NAC Profiler UI. Clicking the Server link in the System Status table will open the Configure Server form so that the current configuration can be viewed and changed as required.

Note If the Server module of a newly configured Cisco NAC Profiler system indicates a status of 'not running', it is likely that the required license files have not been uploaded. Refer to the licensing upload/verification procedures outlined in Chapter 5, "Configuring the Cisco NAC Profiler for the Target Environment"to upload valid licenses and get the NAC Profiler Server status to "running" before proceeding with Profiler Server configuration.

The Configure Server form is organized into several sections containing configurable parameters that are used to configure system-level features and functions of the NAC Profiler System.

When performing the initial configuration of a new NAC Profiler System, the first section at the top of the form entitled Network Connections is the **only** section of the Profiler Server configuration that must be configured to begin NAC Profiler system operations. On a newly installed system, the Network Connections section of the Configure Server will appear as illustrated in Figure 6-1.

Figure 6-1 Configure Server Form: Network Connections Section

Tip Adding appropriate Network Connections to the Profiler Server configuration is essential before the addition of Collectors to the system configuration. When performing the initial configuration of a new NAC Profiler installation, follow the procedures outlined in the next section to add the necessary Network Connections so that network communications between the NAC Profiler Server and NAC Profiler Collectors is enabled, then proceed with the adding of the Collectors to the Cisco NAC Profiler configuration as described in Chapter 7, "Configuring Collector Modules".

Server Network Connection Options on Cisco NAC Profiler Systems

As initially outlined in Chapter 4, "Installation and Initial Configuration" inter-module communications over the network between the Forwarder component module running on a NAC Profiler Collector and the NAC Profiler Server (or HA-pair) can be configured to operate in one of two ways:

- The Forwarder on the Collector can be configured to initiate the connection with the Server (e.g., Network Connection Type of 'Client' on the Collector Forwarder module connecting to a 'Server' Network Connection on the NAC Profiler Server).
- The Forwarder on the Collector can be configured to listen for connections initiated by the Server (e.g., Network Connection Type of 'Server' on the Collector Forwarder that listens for Client connections from the NAC Profiler Server).

Note If the Collector service is running as an HA-pair deployed on HA NAC Servers, the second option (Forwarder configured with Connection type of Server) is required.

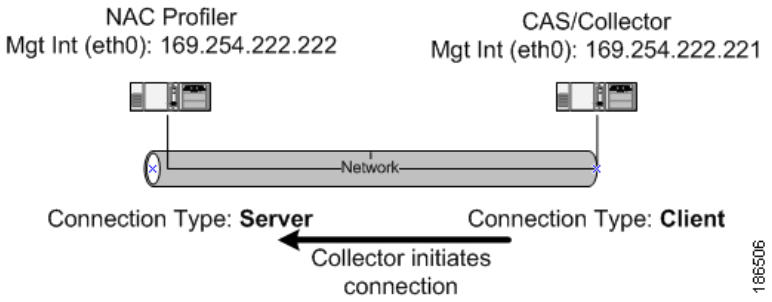
The required Network Connections for a NAC Profiler Server (or NAC Profiler Server HA-pair) are determined primarily by the network environment and configuration of the NAC Profiler Collectors. The following guidelines are provided in the selection of the connection configuration between the NAC Profiler Server and the Collectors in a NAC Profiler System:

- The most common configuration for standalone (non-HA) Collectors is setup of the Forwarder so that it initiates the connection with the NAC Profiler Server. This requires a Network Connection of type 'Server' on the NAC Profiler Server which can support connections from multiple Collectors configured with Network Connections of type 'Client.'
- Collectors running in HA mode on NAC Server HA-pairs **must** have their Forwarders configured to listen for connections initiated by the NAC Profiler Server (via Network Connections of type 'Client'). This enables the connection to the HA Collector pair to be via the VIP so that only the Primary node of the Collector pair is communicating with the NAC Profiler Server at any given time. This requires a Network Connection of type 'Client' be configured on the NAC Profiler Server for each Collector configured in this manner.
- As an option, standalone Collectors that are deployed behind firewalls may also have their Forwarders configured to listen for connections initiated by the NAC Profiler Server. This may alleviate the need for creation of firewall rules allowing the connection from outside the firewall between the Collector and the NAC Profiler Server.

In Cisco NAC Profiler deployments where one or more of the Forwarder modules on the Collectors in the system have been set up with Client configurations (valid for standalone (non-HA) Collectors only), the Server module will require the addition of a Network Connection, with Connection Type of Server, specifying the management interface (eth0) for standalone NAC Profiler Servers, or the VIP for Profiler Server HA-pairs.

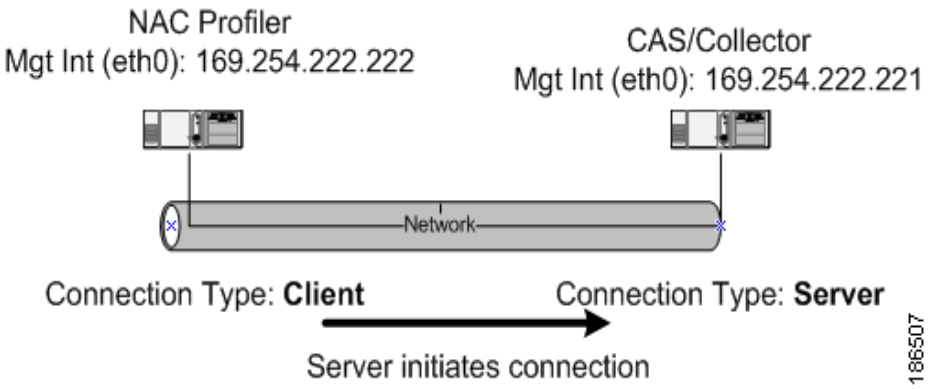
Adding a Network Connection of type Server to the Profiler Server configuration results in the Server listening on the specified TCP port (31416 by default) for network connections by the Forwarder(s) in the system configured to be clients connecting back to that Server module. Figure 6-2 illustrates communications between the Profiler Server via a Network Connection of type Server, and a Forwarder module on a Collector when the Forwarder is configured as with a Network Connection type of Client.

Figure 6-2 Client Network Connection on Forwarder



In deployments where one or more Collectors have their Forwarder configured with Network Connection of type 'Server' (required for Collector HA pairs or firewall traversal) and are relying on the Server module to initiate the connection, a Network Connection with Client Connection Type must be added to the Server module configuration for **each** Collector configured in this manner. Figure 6-3 illustrates communications between the NAC Profiler Server and a Collector when the Forwarder is configured with a Network Connection of type Server. Again, this is the mandatory configuration for Collectors running on NAC Server HA-pairs as outlined in Chapter 4, "Installation and Initial Configuration".

Figure 6-3 Server Network Connection on Forwarder



Follow the procedures in the following two sections for adding the necessary Network Connections to the Server module configuration in order to support the Collectors deployed in the NAC Profiler system and initially configured as outlined in Chapter 4, "Installation and Initial Configuration".

Add Network Connection to Profiler Server Configuration of Type 'Server'

Tip Server type Network Connections added to the Profiler Server configuration result in the Profiler Server listening for inbound connections from Collectors on the specified interface. They provide connectivity for one or more NAC Profiler Collectors configured with a Network Connection of type 'Client.'

To add a new Network Connection of type Server to a Profiler Server configuration, complete the following steps:

Step 1 Select the Add Connection button in the Network Connections section of the Configure Server form. The Add network client/server form that allows specifying the configuration parameters of the Network Connection to be added to the Server module configuration is displayed. See Figure 6-4.

Figure 6-4 Add Network Client/Server Form (Server)

This form allows the specification of each of the required parameters of the Network Connection being added to the Server module configuration which will enable bidirectional communications between the Server and one or more Collectors to initiate communications with the Profiler Server (e.g., Forwarder configured with Network Connection of type Client).

Step 2 Set the Connection Type to Server by ensuring the Server radio button is selected (default).

Step 3 Enter the listening IP Address (interface) for inbound connections from Collectors.

For Standalone NAC Profiler Servers, enter the host IP address of the management interface (eth0) of the Profiler Server appliance.

If the Profiler Server is implemented as an HA-pair, the IP address specified for a Network Connection of Type 'Server' should be that of the VIP assigned to the HA-pair. This ensures that the Collectors utilizing the connection will maintain connectivity with the Server regardless of which appliance is currently the Primary node in the NAC Profiler pair.

For example, if the Management interface of the Profiler Server appliance was assigned the address 169.254.222.1, adding a Network Connection with this address specified would result in the Server module listening for TCP connections on the specified port number on the Management interface (eth0) of the appliance. Remote modules would be able to communicate with the Server by initiating TCP connections to the IP address of the Management interface of the appliance running the Server.

Tip A single Network Connection with Connection Type of Server added to the NAC Profiler Server configuration will support connections from multiple Collectors with Forwarders configured with Client network connections on the default TCP port of 31416. Server module Network Connections are considered as "one-to-many."

Step 4 Specify the TCP Port for the Connection

For most cases the default TCP port number of 31416 should be accepted, however as an alternative TCP port 31417 may be specified. This is the port number that the Network Connection being added will utilize for module-to-module communications.

Step 5 Specify the Encryption Type (default is AES)

Select the desired encryption type for the Network Connection being added from the drop-down list: AES, Blowfish or None. This parameter specifies either that the Network Connection will be unencrypted (select the None option), or the algorithm to use for encrypting the data being transmitted. Currently available encryption options are AES (default) and Blowfish. The Network Connection of the modules at both ends of the Network Connection must have the same encryption algorithm selected in order for encrypted session to be successfully established.

Step 6 Specify a Shared Secret for

Specify the shared secret that should be used in establishing encrypted communications over the Network Connection to be added, if desired. The field should be left blank if the Network Connection will be unencrypted. The modules at both ends of the Network Connection must be configured with the identical Shared Secret in order for the encrypted session to be established successfully.

Tip The Collector service is configured at startup with the parameters the Forwarder module will use in communications with the NAC Profiler Server including Connection Type, Encryption Type, Shared Secret and address information. This enables bidirectional communication with the Server module for the system so that the Collectors are able to get their detailed configuration from the Server. It is good practice to plan and document these parameters for the entire system at the outset of system configuration to ensure system-level communication can be established efficiently.

Step 7 Select the Add Connection button to save the new Network Connection to the Server Configuration, and return to the Configure Server from, which should now display the Network Connection just added.

If additional Network Connections are to be added to the Server module, utilize the procedures in this section or the next to add additional entries as required, then save the changes as described in Saving Added Network Connections to the Server Module Configuration, page 6-9.

Add Network Connection to Profiler Server Configuration of Type 'Client'

Note When configuring a system with multiple "Client" connections (e.g., multiple Collectors configured with Network Connections of type Server to support Collector HA-pairs or firewall traversal), a Network Connection for each of the Collectors the Profiler Server will initiate a connection with is required in the Server module configuration. Unlike Server Network Connections, Client Network Connections on a Profiler Server are "one-to-one."

To add a new Network Connection of type Client to a Profiler Server configuration, complete the following steps:

Step 1 Select the Add Connection button in the Network Connections section of the Configure Server form. The Add network client/server form that allows specifying the configuration parameters of the Network Connection to be added to the Server module configuration is displayed.

Step 2 Select the Connection Type Client radio button.

When the Client radio button for Connection Type on the Add Network Client/Server form is selected, the form changes subtly as shown in Figure 6-5 and Figure 6-6. Figure 6-5 is taken from a standalone NAC Profiler system, Figure 6-6 taken from an NAC Profiler HA-pair.

Figure 6-5 Add NAC Profiler Server Client Network Connection - Standalone

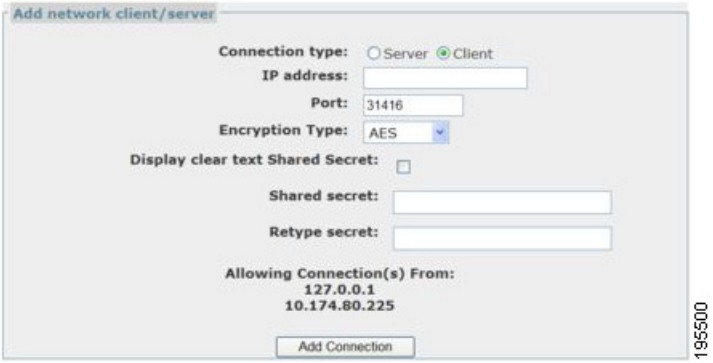
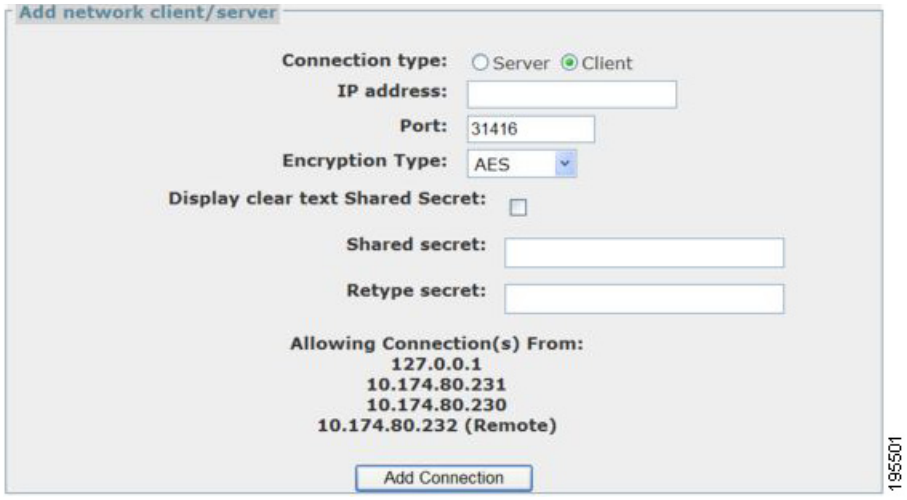


Figure 6-6 Add NAC Profiler Server Client Network Connection - HA Pair



The primary difference in the Add network client/server for the Client connection type is the section immediately above the Add Connection button, entitled “Allowing Connection(s) From:”.

For standalone NAC Profiler Servers, this section lists two IP addresses. In the case of systems with an Cisco NAC Profiler deployed as a HA-pair **four** IP addresses are displayed in the list.

The addresses in the "Allowing Connections From" section of the form are used in the construction of the configuration file for the downstream Forwarder module on the collectors that the NAC Profiler Server will initiate network communications with via the Client Network Connection being added. They are used in the configuration of the Access Control List (ACL) in the Forwarder module configuration so that it only accepts connections from the NAC Profiler Server.

Tip The addresses and should be verified against those configured during the startup of the Collector when they were configured with a corresponding Server Network Connection in accordance with the procedures specified in Chapter 4, "Installation and Initial Configuration".

In the standalone case, the Server will connect to the Collector service using this client connection, initiating the connection using the management interface (eth0) IP address. The loopback address is included as well for completeness.

For HA-pairs, outbound connections from the virtualized Server module may at different times utilize the IP address of the management interface (eth0) of either of the members in the pair dependent upon which appliance is currently the Primary node, or the VIP. The list then should include:

- The management interface(eth0) IP address of the Primary appliance
- the management interface (eth0) IP address and Secondary appliance
- the VIP of the HA-pair
- The loopback address (127.0.01).

Step 3 Enter the IP Address for the Client network connection.

For Connection Types specified as "Client" the IP address entered should be the IP address of the remote Collector the Server module will initiate communications with. For example, when adding a Network Connection to a Server module to establish communication with a Forwarder module on a Collector, specify the IP address of the management interface (eth0) of that Collector service, in this field. If the Collector is deployed on an HA NAC Server pair, the VIP of the NAC Server pair should be entered.

Step 4 Enter the TCP Port to be utilized for this connection.

For most cases the default TCP port number of 31416 should be accepted, however an alternative available layer 4 port values may be specified. This is the port number that the Network Connection being added will utilize for module-to-module communications.

Step 5 Enter the Encryption Type

Select the desired encryption type for the Network Connection being added from the drop-down list. This parameter specifies either that the Network Connection will be unencrypted (select the None option), or the algorithm to use for encrypting the data being transmitted. Currently available encryption options are AES (default) and Blowfish. The Network Connection of the modules at both ends of the Network Connection must have the same encryption algorithm selected in order for encrypted session to be successfully established.

Step 6 Specify the Shared Secret

Specify the shared secret that should be used in establishing encrypted communications over the Network Connection to be added, if desired. The field should be left blank if the Network Connection will be unencrypted. The modules at both ends of the Network Connection must be configured with the identical Shared Secret in order for the encrypted session to be established successfully.

The form requires the shared secret to be entered identically two times to prevent mistakes in typing the desired string.

Note The Collector services are configured at startup in accordance with Chapter 4, "Installation and Initial Configuration", with the parameters they require such as Connection Type, Encryption Type, Shared Secret and address information as required to complete the configuration of the Forwarder end of the communication. This enables bidirectional communication with the Server module for the system so that the Collectors are able to get their detailed configuration from the Server.

Saving Added Network Connections to the Server Module Configuration

When all required Network Connections have been added to the Server Module configuration, select the Update Server button at the bottom of the Configure Server form. Then perform an Apply Changes -> Update Modules to generate the new Server configuration file and restart the Server using the configuration with the added Server module Network Connections so that they are ready for use when the Collectors are added to the system configuration as described in Chapter 7, "Configuring Collector Modules".

Editing Other Server Configuration Parameters

Tip When completing the initial configuration of NAC Profiler Server, the only mandatory configuration task is adding appropriate Network Connections to enable network communications between the NAC Profiler Server and the Collectors as outlined in the previous sections of this chapter. Remaining parameters of the NAC Profiler Server can be revisited later and configured in accordance with the guidance provided in this section, or other chapters in the case of NAC Appliance and LDAP integration features. For newly installed systems, it is best practice to proceed with the addition of the Collectors to the system configuration as described in Chapter 7, "Configuring Collector Modules".

In addition to the Network Connections configuration of the NAC Profiler Server, there are several other sections of the Configure Server form that allow the setting of parameters that control system-level operation of the system.

Database Maintenance

The Database Maintenance parameters of the Profiler Server configuration are immediately below the Network Connections section of the Configure Server form. Figure 6-7 is an excerpt from a newly installed NAC Profiler Server showing the default settings for the parameters in this section.

Figure 6-7 Configure Server: Database Maintenance Parameters

The Database Maintenance parameters allow the setting of a number of timeouts that control how endpoint data is retained or purged by the system. The paragraphs below outline the purpose of each of these parameters:

Tip If the Profiler Server timeout parameters are left at the default (no timeouts enabled), all endpoints that are discovered by the system will remain in the database indefinitely. Although their historical data will be pruned (30 days by default), the endpoints themselves will remain in the primary endpoint console views (View endpoint by profile, etc.) unless removed manually (one at a time) via Clear Endpoint. As described below, the Endpoint Timeout and Endpoint Removal parameters can be used to automatically clear the database of endpoints that have not had data collected for a defined period of time, pruning the database of endpoints that are no longer connecting to the network.

Tip The timeout parameters outlined below are applied by the system on a per-Profile basis: only endpoints in a profile that has the "Allow Timeout" parameter set to 'yes' will be effected by the timeouts as described below. Endpoints in the "Not Profiled" state are **always** (not configurable) subjected to the timeouts configured for the Server module.

Endpoint Timeout

The Endpoint Timeout can be used to prune the endpoint database in the NAC Profiler system of endpoints that are inactive, presumably having left the network permanently. The endpoint database can be conceptualized as being organized by the MAC address and containing all the endpoints the system has discovered and observed identity attributes (e.g., endpoint profiling data) for. For each endpoint MAC discovered, Cisco NAC Profiler maintains both MAC-learned and IP-learned profiling about that endpoint. When any observation of the endpoint from the Collectors is observed, a timestamp for that data element is updated so that each element of endpoint data in the database for each endpoint has an age, so that the endpoint database can be managed by the system actively. The endpoint timeout is used to manage if or when endpoints that don't have any updates to their profiling information are moved to an inactive or "retired" status.

When this timeout is set to other than the default of 0 days (interpreted as "don't retire any endpoint regardless of how long it has gone without update to its data"), if no endpoint data has been observed by the system within the number of days specified the endpoint is moved to a "retired" state. As an endpoint is moved to the retired state, the following changes are effected within the system:

1. Retired endpoints are removed from the primary Endpoint Console views: the Endpoint Directory, and Display Endpoints by Profile/by Device Port. Endpoints in the retired state can only be viewed from the Endpoint Console tab by selecting Other Endpoint Views -> Retired Endpoints.
2. As an endpoint is moved to the retired state, if it is in a Profile that matches a NAC Event or the profile is 'LDAP enabled,' the endpoint is removed from the CAM Filter List and the LDAP directory respectively—the endpoint is essentially considered to be inactive for the purposes of integration with other systems. If the endpoint was enabled for MAC authentication via these mechanisms, it is essentially revoked and the endpoint must be rediscovered and profiled as described below.
3. All endpoint profiling data for the endpoint is cleared (both IP- and MAC-learned) along with current IP-to-MAC mapping and endpoint location information. If the endpoint becomes active again, it will be treated the same as a new endpoint being discovered by Cisco NAC Profiler for the first time (with the exception of the historical data as outlined in #d. below). That is, the system would have to collect identity attributes and profile the endpoint according to the data collected after re-discovery.

4. Endpoints that have been retired will have their historical information retained subject to the historical limit as described below. MAC history by port, MAC history by IP, and MAC history by Profile for the endpoints in retired status is maintained in the database subject to the historical limit parameter (30 days by default). Should the endpoint return to the network and the endpoint moved out of the retired state, its historical information will be rejoined with the current data for the endpoint.

Endpoint Removal

The Endpoint Removal timeout is used in conjunction with the Endpoint Timeout. Endpoint Removal specifies the number of days an endpoint is maintained in the "retired" status as described above. If the endpoint removal parameter is set to a number of days other than the default of 0, endpoints will remain in the retired state for only the number of days specified. Retired endpoints subjected to endpoint removal timeout are permanently removed from the Cisco NAC Profiler database—no information about the endpoint is retained. When an endpoint is subjected to the Endpoint Removal timeout the effect is similar to the Clear Endpoint functionality (see Chapter 15, “Using the Cisco NAC Profiler Endpoint Console”) that allows individual endpoints to be selected for permanent removal from the database, but in the case of endpoint removal, happens automatically to any number of endpoints that have been in the retired state greater than the value selected for this parameter. This provides an automated database pruning functionality.

Tip It is worth reemphasizing that in order to subjected to any timeout, endpoints must either be in a profile that has the "allow timeout" parameter enabled or be in the Not Profiled state as the system evaluates the age of their profiling data. If endpoints are not in a Profile that has "allow timeout" enabled or are Not Profiled, they will not be subjected to Endpoint Timeout/Endpoint Removal.

Port Timeout

The Port Timeout value is used to clear location (access switch and port) information for individual endpoints. The location information for endpoints is determined by Cisco NAC Profiler via NetMap, and the NetTrap trap handling mechanisms. The normal trap handling mechanism operates as follows when endpoints are physically removed from the network: the access network device (switch typically) will generate a link down trap which is processed by NetTrap. On receipt of link down, NetTrap informs the Server which in turn commands the NetMap module to poll the device port via SNMP to verify that the MAC has in fact been removed (is no longer in the switch source address table). Upon that confirmation, that location information is cleared for the endpoint and Cisco NAC Profiler is unable to provide a current location for the endpoint. The default value is 0, meaning the this timing mechanism will not be used.

In scenarios where endpoints are learned on ports via the NetMap mechanism and that location information is added to the database for the endpoint, and the endpoint subsequently disconnects from that location but no link down trap is generated/processed by NetTrap, the location information cannot be cleared automatically for the endpoint by the NAC Profiler system. This can happen in a number of scenarios such as endpoints connected via the switch integrated in IP Phones which do not support traps/are not polled, or through wireless Access Points which result in Cisco NAC Profiler locating them on the upstream wired switch. The port timeout can be used to semi-automatically cull stale endpoint location information, typically generated when endpoints are connected to the network via these methods.

By default this timer is set to 0 specifying that location information for endpoints will not be timed out via this mechanism, and that only positive indications of leaving the network will trigger the removal of location information for endpoints.

ARP Timeout

The ARP timeout specifies how long the IP-to-MAC mapping will be retained for an endpoint without refresh of that data. By default, this parameter is set to 0 (hours) interpreted as the last IP-to-MAC mapping determined by the system will not be cleared by timeout. Cisco NAC Profiler strives to maintain an IP-to-MAC mapping for each endpoint that it learns through a number of collection mechanisms: NetMap polling of router ARP caches, monitoring of DHCPAck packets from DHCP servers, and NetWatch processing of ARP transactions.The IP-to-MAC mapping enables learning of endpoint identity attributes via analysis of the endpoint's network traffic (or NetFlow XDRs) which identify the endpoint only via IP address.

If the ARP timeout is left at zero, the last IP-to-MAC mapping determined by Cisco NAC Profiler using the mechanisms above is maintained indefinitely. For non-zero values, endpoints that have not had a refresh of IP-to-MAC information within the specified number of hours will have their current IP-to-MAC mapping cleared.

Implications of clearing IP-to-MAC mappings for an endpoint need to be well understood as this parameter is implemented. In order for IP-learned information to be tagged with an endpoint MAC address making it persistent through IP-to-MAC mapping clearing and changes of IP for the endpoint, the MAC-to-IP binding has to have been learned either through the observation of a complete DHCP transaction (including DHCPAck from DHCP Server) or a complete ARP transaction. If the IP-to-MAC mapping was made only via the NetMap mechanism (finding an ARP cache entry for the endpoint MAC in a network device), clearing of the IP-to-MAC mapping for the endpoint, or an observed IP address change will result in the purge of IP-learned profiling data for the endpoint. This may result in a profile change for the endpoint.

Historical Limit

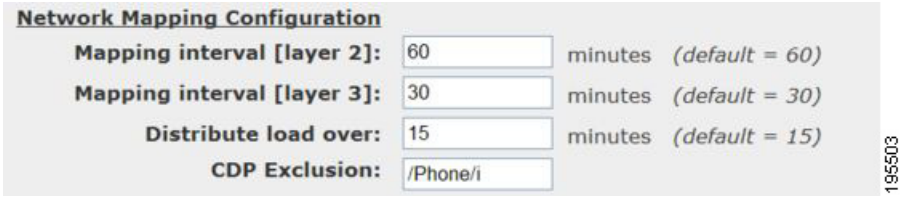
Specifies how long historical information for endpoints is maintained by the system for endpoints discovered by Cisco NAC Profiler. As described above, Cisco NAC Profiler retains historical information (MAC history by port, MAC history by IP, and MAC history by Profile) for each endpoint it discovers by MAC address, whether the endpoint is currently in an active or retired status. This value specifies the time horizon for retention of this historical data. The system will automatically clear endpoint historical data older than the specified value which keeps the database size bounded, particularly in cases where the Endpoint Timeout/Endpoint Removal mechanisms are not used.

Note Changes to any of the above timeout values on a running system requires that an Apply Changes -> Update Modules be executed in order for the change to be committed to the running configuration. It may take up to 1 hour for the newly-enabled timeout values to take effect, it will not be instantaneous.

Network Mapping Configuration

The parameters in this section set configurable parameters for all NetMap and NetTrap modules across the system. This section of the Configure Server form is illustrated in Figure 6-8

Figure 6-8 Configure Server: Network Mapping Configuration



The configurable NAC Profiler Server parameters in this section are outlined in the following sections:

Mapping Interval [Layer 2]

This parameter defines how often (in minutes) the NetMap component module(s) running on the NAC Profiler Collector(s) will poll Layer 2 devices (switches) for all device information via SNMP. (Default is 60 minutes)

Mapping Interval [Layer 3]

This parameter defines how often (in minutes) the NetMap module(s) running on the NAC Profiler Collector(s) will poll Layer 3 devices (routers) in the database for information via SNMP. (Default is 30 minutes).

Distribute Load Over

Specifies a time value (in minutes) over which to distribute the SNMP polling of network devices in the system configuration. The NAC Profiler system will allocate the SNMP polling of network devices in its configuration over a defined period of time to make efficient use of NAC Profiler system and network resources. This value specifies the time period over which that distribution should occur. The default value is 15 minutes.

The number of network devices in the configuration is divided by the value of this parameter to determine how many devices will be polled each minute by the NetMap module(s) in the system. The NetMap module(s) will in turn spawn a worker for each device to be polled. If the number of devices is greater than the Maximum allowed workers as specified in the NetMap module configuration (see Chapter 7, "Configure NetMap Collector Module" section on page 7-12), NetMap will queue these requests. If the Distribute Load Over parameter is set to 1 all devices will be polled simultaneously.

The following example shows how this calculation is made for a given NAC Profiler system with 60 network devices in the configuration, with this parameter set to the default value of 15 minutes and a single Collector (NetMap module).

Example:

Network Devices in the configuration = 60

Distribute Load Over value = 15

Devices per Bucket = (60/15) = 4

Therefore at the top of each minute for a total of 15 minutes, 4 XML requests are sent to the NetMap module, initiating 4 NetMap workers, each worker polling a single network device. The total time to complete SNMP poll of all devices is therefore 15 minutes.

CDP Exclusion

The NAC Profiler system uses the CDP protocol for the identification of trunk ports on network devices. When it is determined that a device that identifies itself to its upstream neighbor via CDP, by default NAC Profiler will designate the port as a trunk port. The designation is used in the UI to control the display of MAC addresses on a port. Trunk ports will not show the MACs of endpoints present on the trunk port. There are cases however where that is not desirable; that the presence of a CDP-enabled device downstream should not result in the port being treated as a trunk, it is still in fact an access port providing connectivity to a single device. The most common example of course is an IP Phone, which identifies itself as a phone in its CDP message.

This parameter allows adding additional exclusions to the default of “phone” that prevents trunk determination via CDP. The exclusion list is defined as a Regular Expression which can contain multiple strings that result in the system ignoring CDP messages in its determination of trunk ports.

For example, if IP Video cameras were present on the network in addition to IP Phones, and those cameras used CDP to identify themselves to their upstream neighbor with the string “camera” in the CDP Message, changing the CDP Exclusion Regular Expression to:

```
/phone|camera/i
```

Would result in NAC Profiler not marking ports that provide connectivity to IP phones or cameras that use CDP as trunks in the UI so that the endpoints MACs located by Profiler on that port will be displayed in the Cisco NAC Profiler UI.

Trust Cisco MAC Notification Trap

This parameter, enabled by default, allows the configuration of the system to accept endpoint information contained in Cisco MAC notification traps without verification of the port information via SNMP polling by NetMap after receipt of a trap (default trap handling behavior).

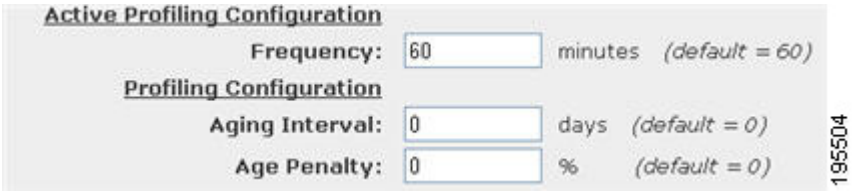
If checked, the system will not command an SNMP poll of the switch via NetMap for bridge MIB information upon receipt of a Cisco MAC notification trap; it will add/update information for the endpoint MAC using the information contained within the trap, polling the trapping network device only for PAE MIB information.

Tip The Trust Cisco MAC Notification trap options can significantly reduce the amount of SNMP polling performed by the system. However, it is highly recommended that this feature only be used on systems that have the Community String verification option enabled for the NetTrap module(s). See Chapter 7, “Configuring Collector Modules” for instructions on the configuration of NetTrap and the community string verification option.

Active Profiling Configuration/Profiling Configuration

The parameters in this section set configurable parameters for Active Profiling and Profile Data aging across the system. This section of the Configure Server form is illustrated in Figure 6-9

Figure 6-9 Configure Server: Active Profiling/Profiling Configuration



The configurable parameters in this section are outlined in the following sections:

Active Profiling Frequency

Specifies the polling interval (in minutes) the NetInquiry module(s) running on the NAC Profiler Collectors will perform their active profiling function. (Default is 60 minutes).

See Chapter 7, "Configure NetInquiry Collector Module" section on page 7-21 for information regarding NetInquiry, and Chapter 10 "Profile Rules, NetInquiry and Active Profile Data Collection" section on page 10-30 for an in-depth discussion of both the NetInquiry module and the Active Profiling capabilities of the NAC Profiler System.

Note Active Profiling frequency is a system-wide parameter. If one or more NetInquiry modules are configured/enabled on the system with DNS Collection enabled, and or active TCP Open Port or Banner rules present in enabled profiles, the NetInquiry module(s) are going to perform this function at the selected frequency which *may* cause a large load on the NAC Profiler system, network and DNS system. Strong consideration should be given to adjusting this parameter accordingly prior to configuring/enabling Active Profiling on the system.

Profiling Configuration Aging Interval and Aging Penalty

These optional parameters are used to age the individual Profiling data elements gathered by the NAC Profiler system about an endpoint over time. Each element of Profiling data about an endpoint observed by NAC Profiler is tagged with a time-based confidence value which is set to 1.0 the first time the data is seen, and reset to that value each time NAC Profiler observes the endpoint identity attribute. The parameters below specify how each of the individual Profiling data elements will be timed-out by NAC Profiler if they are not re-observed within a defined period of time.

Aging Interval

Specifies a time value (in days) to wait for a refresh before the system will decrement the confidence value for each endpoint profiling data element.

Age Penalty

Specifies a value (%) to decrement the confidence value with the expiration of an Aging Interval without a refresh of Profiling data.

For example, if a DHCP request from an endpoint was observed by NAC Profiler at time = 0, that DHCP data element would be tagged with a confidence value of 1.0 (100%). If an Aging Interval was set to 4 days, with an Age Penalty of 25% and another DHCP request was not observed by NAC Profiler for four days, the confidence value of that data element would be decremented from 100% to 75%. If no DHCP request was observed for 4 Aging Intervals (e.g., 16 days), then the DHCP information would have a confidence value of 0, and that information would no longer be used for Profiling that endpoint.

Tip In the current version, the effect of the timing out of endpoint data elements by the use of this parameter is only made upon execution of an Apply Changes -> Update Modules or Re-model when the database is remodeled manually. This functionality will not result in dynamic re-profiling of endpoints as individual data elements are aged out.

LDAP Configuration

The LDAP Configuration section is optional and specific to environments where the LDAP integration capability will be utilized to integrate NAC Profiler with RADIUS authentication servers such as Cisco Secure ACS. See Chapter 17, "Enabling LDAP Integration"for detailed instructions for using the NAC Profiler LDAP functionality.

External Reference

The External Reference parameter is used by the NAC Profiler System for two purposes:

1. Identifying the NAC Profiler system when sending SNMP traps to external systems for NAC Profiler Event Delivery, see Chapter 12, "Configure Cisco NAC Profiler Events".
2. Identifying the NAC Profiler system when communicating with the Cisco NAC Appliance NAC Server for systems integrated with NAC Appliance. See Chapter 13, "Integration with Cisco NAC Appliance"

NAC Integration

The External Reference and NAC Integration parameters are required for integration of Cisco NAC Profiler with Cisco NAC Appliance. See Chapter 13, "Integration with Cisco NAC Appliance" of this guide for detailed instructions on the use and configuration of these Server module parameters.

SNMP Configuration

The SNMP Configuration Profiler Server parameters contains optional configuration parameters and is utilized as desired for configuration of the NAC Profiler Server to send information to the NMS via SNMP traps. There are no default values for these parameters.

Instructions for the use of these parameters for configuration of the Profiler Server to deliver NAC Profiler events via SNMP traps is outlined in Chapter 12, "Configure Cisco NAC Profiler Events".

HA Warning Threshold for Queued Rows (Cisco NAC Profiler HA pairs Only)

On NAC Profiler Server HA pairs only, an additional Profiler Server configuration parameter is included, the HA Warning Threshold for Queued Rows.

On NAC Profiler Server HA-pairs, an early warning algorithm is implemented to warn the administrator when database synchronization on the Secondary node is falling behind.

This parameter specifies the number of rows of pending database synchronization changes to be made on the Secondary node that can be queued before indications of a potential HA failure is indicated by the UI.

In most Profiler Server HA pair implementations, the default value of this parameter provides timely warning without false positives. However, in very large and dynamic systems, this threshold may be too low and will require upward revision to accommodate very heavy synchronization activity.

Prior to adjusting this value, consultation with Cisco technical support is recommended.

Saving Edits to the Cisco NAC Profiler Server Configuration

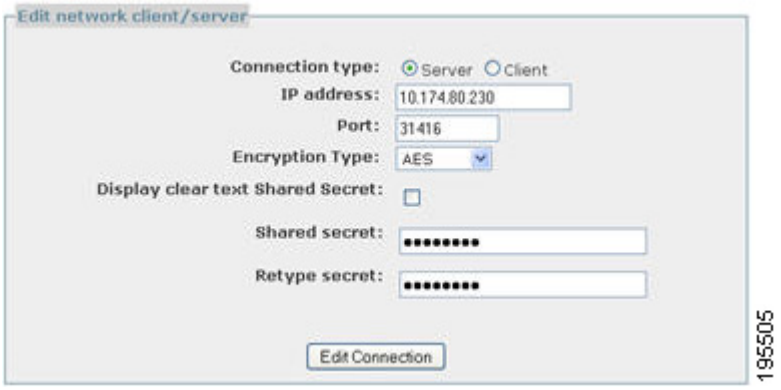
When all desired changes have been made to the configuration of the N AC Profiler Server, select the Update Server button at the bottom of the Configure Server form. Selecting the Update Server button results in the browser returning to the Table of Modules page, and a message displayed at the top of the main pane that the Profiler Server configuration has been saved.

The changes to the Server module configuration are not committed to the running configuration until the Apply Changes -> Update Modules procedure is performed as described at the end of Chapter 5, "Configuring the Cisco NAC Profiler for the Target Environment".

Editing a Profiler Server Network Connection Previously Added to the Configuration

To edit an existing Network Connection in a Server module configuration, navigate to the Configure Server form, select the Edit radio button to the right of the Network Connection to be edited. Then select the Edit Button. The Edit network client/server form is displayed which reflects the current configuration and allows each of the Network Connection parameters to be edited as required (see Figure 6-10). Refer to Saving Edits to the Cisco NAC Profiler Server Configuration, page 6-17 for a description of each of these parameters for Network Connections of type Server and Client to be configured on a NAC Profiler Server.

Figure 6-10 Edit Network Client/Server Form



Once the desired changes are made to an existing Network Connection, select the Edit Connection button to save the edits to the configuration, and return to the Configure Server form.

Note Changing the parameters of an existing Network Connection on the NAC Profiler Server will result in the Forwarder module(s) on Collectors currently communicating on that connection to be updated as well. In the case of Collectors running in HA mode on NAC Server HA-pairs, only the Primary node will have its Forwarder module re-configured as only the Collector service on the Primary node is in communication with the Server. The Secondary node will need to be re-configured manually from the command line so that upon failover, it has the correct configuration parameters to maintain communication with the Profiler Server.

Removing a Profiler Server Network Connection

To remove a Network Connection from a Server module configuration, select the Remove checkbox to the right of the Network Connection or Connections to be removed. Selecting the Remove button will result in the removal of the selected Network Connection or Connections from the Profiler Server configuration.