CHAPTER 7

Configuring Cisco NAC Collector Modules

This chapter includes the following topics:

Overview

The NAC Profiler Collector modules, collocated on the CAS appliances in Cisco NAC Profiler are essentially the “eyes and ears” of the system.

Note The Collector must be enabled on the CAS as described in Configuring the Collector on the Clean Access Server, page 4-36.

The five component modules running on the Collector(s): NetInquiry, NetWatch, NetMap, NetTrap and NetRelay collect endpoint information for the system that is processed into the database and analyzed and presented by the NAC Profiler Server. The NAC Profiler Server also updates the NAC Appliance CAM with information about non-NAC endpoints based on the database it maintains using information from the Collectors deployed throughout the system and compiled by the component modules. The component modules each utilize different technologies and techniques for endpoint data collection and analysis, providing a full complement of Endpoint Profiling and Behavior Monitoring capabilities for the system.

Figure 7-1 shows a logical representation of the NAC Profiler Collector and its component modules.

Figure 7-1 CAS with NAC Profiler Collector Diagram (Logical)

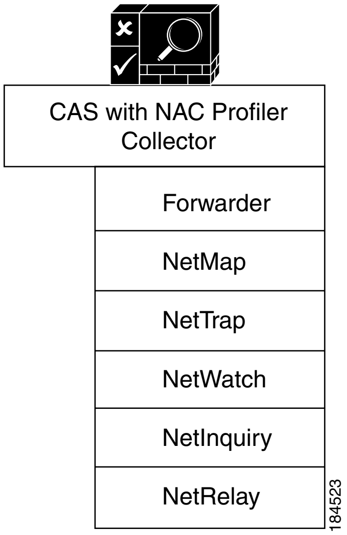


Table 7-1 lists the purpose and functionality of each of the five Collector component modules which can be utilized by each Cisco NAC Collector as required by the implementation:

Table 7-1 NAC Profiler Collector Modules

Module Name	Purpose and functionality
NetMap	SNMP module that queries network devices for the following types of information: • System • Interface • Bridge • 802.1x • Routing and IP
NetTrap	Reports link state changes and New MAC notifications
NetWatch	Passive network traffic analyzer
NetInquiry	Active profiling module that can be used with TCP Open Port and some Application rules
NetRelay	Receives and processes Netflow export packets directly from switches or other Netflow data sources

The component modules used in a specific NAC Profiler system depend on the implementation and environment. In general, a NAC Profiler Collector is deployed on each CAS. The characteristics of the environment, such as the number of endpoint devices, whether or not the network is on a single campus or dispersed across multiple campuses, and how the Endpoint Profiling and Behavior Monitoring functions are implemented determine how the NAC Profiler Collectors are implemented. For example, not all of the component modules in Figure 7-1 are utilized on a given NAC Profiler Collector or used at all for that matter in every deployment. For environments that do not have Netflow collectors running in the network, the NetRelay module is not be utilized in Cisco NAC Profiler for that network.

This chapter outlines the steps required to add and configure each of the NAC Profiler Collectors deployed in a system. For each NAC Profiler Collector deployed, the Collector and its component modules are added to the system configuration via the web interface at initial deployment. Collectors and their component modules in a system configuration can be edited on a running NAC Profiler system at any time by following the procedures outlined later in this chapter. The NAC Profiler web interface enables the status of the Collectors and component modules to be determined at a glance via the Configuration tab option to list/configure Profiler Modules.

As discussed in Chapter 5, "Configuring NAC Profiler for the Target Environment," whenever changes are made to module configuration parameters, an Apply Changes and system restart must be performed to commit the changes to Cisco NAC Profiler running configuration. Upon completion of editing or adding a Collector module or modules to the system configuration, perform an Apply Changes to update the system configuration.

Changes made to NAC Profiler system configuration are saved to the running configuration by clicking the Update Modules button on the Apply Changes page. The Apply Changes page is accessed by selecting the Apply Changes from the global navigation pane in the left hand margin on all pages of the Configuration Tab, or by selecting Apply Changes from the table on the main Configuration page.

Pre-Deployment Considerations for Collectors

In Cisco NAC Profiler the Collector function is co-located on theCisco NAC Appliance providing the Clean Access Server (CAS) services. The way the Collector functions, specifically which component modules are enabled and how they are configured, depends on the specifics of the Cisco NAC Appliance deployment. The most important aspects to take into consideration are:

1. Operating mode of the Clean Access Servers in the systen: Virtual Gateway or Real IP Gateway.
2. In-band or out-of-band (IB or OOB) deployment.

With these two considerations taken together there are four possible Clean Access Server operation modes. These are :

- Real-IP Gateway IB
- Virtual Gateway IB
- Real-IP Gateway OOB
- Virtual Gateway OOB

The choice of deployment model has implications for how the Collector and the underlying component modules are able to gather and process Endpoint Profiling and Behavior monitoring data from endpoints and the network infrastructure. Understanding these implications prior to the deployment and configuration of Collectors is crucial to a successful deployment.

Table 7-2 summarizes the considerations for each of the Collector component modules for each of the four CAS operation modes. For several of the component modules, specific data collection functions are called out for emphasis. A 'Y' in the column for each of the operational modes indicates that the collection function is available with any caveats indicated by the note(s). 'Selective' indicates that the collection function is available but subject to certain limitations that are outlined in the notes.

Review Table 7-2 and the corresponding *Release Notes for Cisco NAC Profiler* when planning the deployment of the Collector(s) employed by Cisco NAC Profiler prior to beginning the Collector configuration steps outlined in the remainder of this chapter.

Table 7-2 *Collector Modules and NAC Appliance Server Operating Mode*

Collector Module / Function	Clean Access Server Operating Mode Real-IP Gateway	Virtual Gateway	Real-IP Gateway OOB	Virtual Gateway OOB
NetMap SNMP polling of switches and routers	Yes	Yes[1]	Yes	Yes [1]
NetTrap Receive SNMP traps from switches	Yes	Yes [1]	Yes	Yes [1]
NetWatch [2, 3]				
• Observe traffic on eth2 (can be HA heartbeat)	Yes [4]	Yes [4]	Yes [4]	Yes [4]
• Observe traffic on eth3	Yes	Yes	Yes	Yes
NetInquiry Active Profiling of endpoints	Yes	Yes[1]	Yes	Yes [5]
NetRelay Reception of NetFlow Export Data Records	Yes	Yes [1]	Yes	Yes [1]

[1] The CAS/Collector in Virtual Gateway (bridged) mode can reliably contact endpoints/devices via the "untrusted" interface (eth1). However, a Virtual Gateway CAS/Collector cannot communicate with any Layer 2-adjacent device with the exception of its own default gateway via the "trusted" interface (eth0). This means the Virtual Gateway CAS cannot talk to, via its eth0 interface:
-- any host connected to a trusted-side VLAN that is declared in the VLAN mapping table
-- any host connected to a configured trusted-side CAS management VLAN
-- any host connected to the trusted-side native VLAN (i.e. non-tagged traffic being bridged by the Virtual Gateway CAS)

As long as the trusted-side target device is not Layer 2-adjacent, then the CAS can communicate with the device reliably via the eth0 interface. The target device must be separated from the CAS on trusted side by one or more Layer3 routing hops.

The use of dedicated management VLANs for switches and routers (but not the same VLAN as the CAS management VLAN) is a general network engineering best practice that removes this concern for the purposes of both NetMap and NetRelay Collector component modules (and also NetInquiry, for Virtual Gateway In-Band only. For NetInquiry with Virtual Gateway OOB, see [5]).

[2] The NetWatch Collector component module is used to observe endpoint behavior through targeted analysis of network traffic "sniffed" from various sources via any available network interface on the CAS/Collector. However Collector functionality must coexist with CAS functionality. Therefore, not all of the CAS Ethernet interfaces can be used for general purpose monitoring (as detailed in the following notes). NetWatch is typically used:
-- To sniff endpoint traffic via a switch-based port or VLAN monitoring mechanism ("SPAN" or similar), with network traffic directed to the eth3 interface (and/or eth2, for a standalone CAS - see [3]). Refer to *Release Notes for Cisco NAC Profiler* for additional information.

[3] For an OOB deployment, NetWatch can observe the endpoint traffic types only while an endpoint is in the untrusted state (with traffic contained to flow In-Band through the CAS). An endpoint that has completed the OOB logon/posture assessment process no longer sends traffic through the CAS.

[4] When the CAS is deployed as a High Availability (HA) pair, eth2 is typically used for the UDP HA heartbeat connection. When eth2 is used for HA, eth2 is not available for NetWatch. For this reason, Cisco recommends using the eth3 interface of the CAS for general purpose traffic monitoring in most cases.

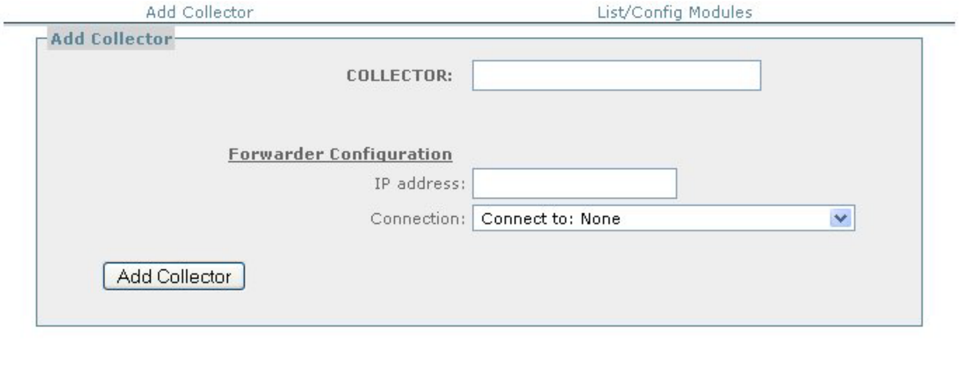
[5] For Virtual Gateway OOB deployments, NetInquiry on the Collector can actively profile endpoints while they are in the untrusted state. When an endpoint becomes OOB connected to an access VLAN, NetInquiry is NOT able to actively profile this endpoint while it remains in this state IF (and only if) the access VLAN is in the CAS VLAN Mapping Table (see [1]). If the endpoint becomes OOB connected via an access VLAN that is not in the VLAN Mapping Table (such that the endpoint is no longer Layer 2 adjacent to the CAS) then NetInquiry can continue actively profiling this endpoint.

Add a NAC Collector to a Configuration

As a new NAC Profiler system is implemented, Cisco NAC Profiler configuration contains no NAC Profiler Collector Module instances. Each of the NAC Profiler Collectors to be deployed in the system must be added to the configuration using the procedure outlined in this section. Adding a new Collector is a two-step process: adding the new Collector to the configuration, and configuring the desired component modules on the newly added Collector as required.

Navigate to the Configuration Tab and select Profiler Modules from the table or the left hand navigation pane. The Configure Profiler Modules page displays. Select the Add Collector link from the table or left hand navigation pane to open the Add Collector form (Figure 7-2).

Figure 7-2 Add Collector Form



Add Collector List/Config Modules

Add Collector

COLLECTOR:

Forwarder Configuration

IP address:

Connection: Connect to: None

The Add Collector form creates a new Collector in the system configuration. All the fields in the form are required, and are described in detail below. Enter this information to add the new Collector to Cisco NAC Profiler configuration.

Collector

This field is used to enter the hostname of the NAC Profiler Collector being added to the configuration.

The hostname of the NAC Profiler Collector entered in this field must match the hostname exactly (e.g., is case sensitive) of the Collector/CAS being added in order for the NAC Profiler to properly establish communications with the Forwarder necessary for reporting status of the component modules running on the Collector.

Forwarder Configuration

The Forwarder Configuration specifies the parameters for communications between this NAC Profiler Collector and the NAC Profiler Server. The parameters specified here should match exactly both those specified when the Collector was installed/initialized and the parameters specified in the Server module configuration (Network Connections section) as outlined in the last chapter.

IP Address

Enter the host IP address of the management interface (eth0) of the CAS hosting the NAC Profiler Collector being added to the configuration.

Connection

This parameter specifies how the Forwarder module running on the NAC Profiler Connector should connect to the Server module on the NAC Profiler Server. Again, this parameter needs to be consistent with both the setup of the NAC Profiler Collector and the Server configuration completed in accordance with the previous chapter.

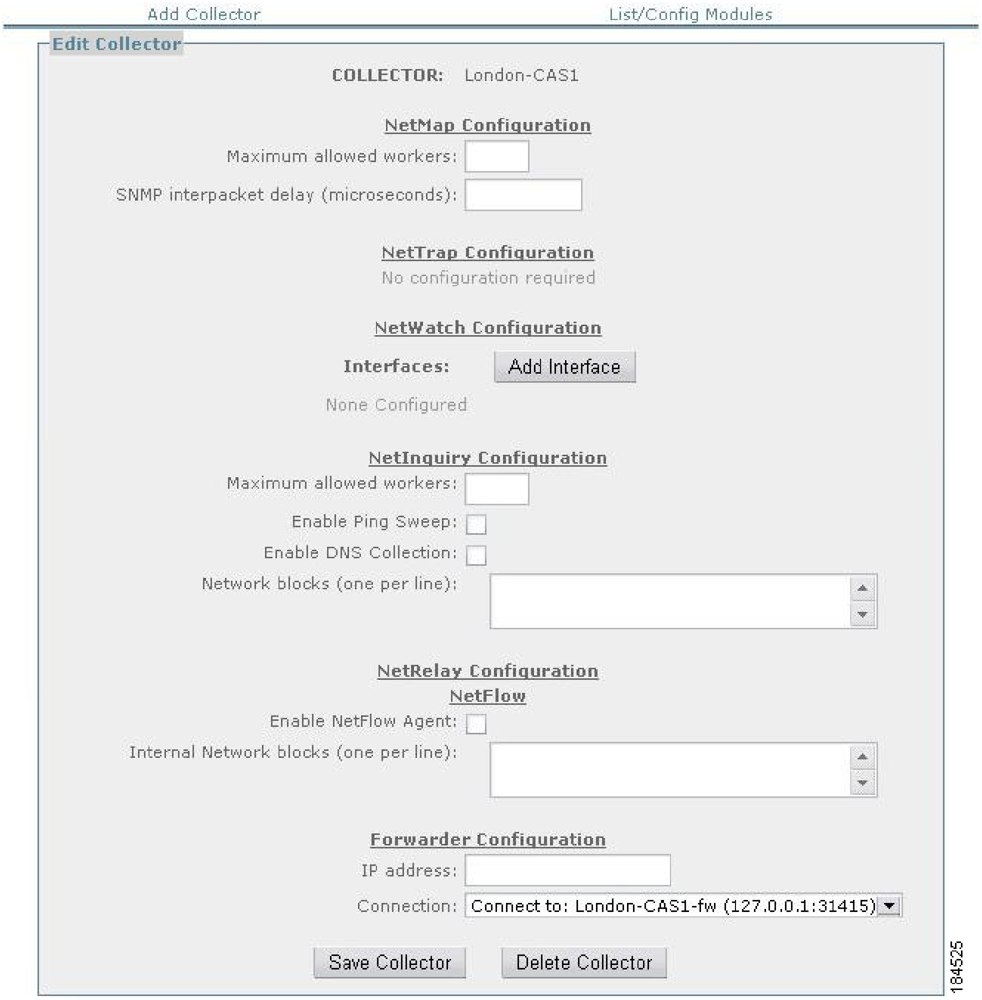
If the connection type was specified on the Collector as ‘**client’** at installation on the CAS (interpreted as the Collector will initiate the connection with the Server), and the Server module has the appropriate Network Connection of the type ‘server’ configured, the proper choice is “Connect to: Server (Server IP: port number).

If the connection type was specified on the Collector as '**serve**r' at installation on the CAS (interpreted as the Collector will wait for initiation of the connection by the Server), and the Server module has the appropriate Network Connection of the type 'client' configured, the proper choice is "Listen for: Server (Server IP: port number)."

Absence of the "Listen for: Server" choice from the drop down list indicates the lack of the client Network Connection configured in the Server module configuration. Review the section in Chapter 6, "NAC Profiler Server Configuration," regarding configuring Network Connections for Servers to support communications with Collectors.

Select the Add Collector button at the bottom of the form to add the Collector to the system configuration. This action adds the Collector and displays the form shown in Figure 7-3 that enables the configuration of the modules running on the NAC Profiler Collector as required by the implementation.

Figure 7-3 Edit Collector Form



COLLECTOR: London-CAS1

NetMap Configuration

Maximum allowed workers:

SNMP interpacket delay (microseconds):

NetTrap Configuration

No configuration required

NetWatch Configuration

Interfaces:

None Configured

NetInquiry Configuration

Maximum allowed workers:

Enable Ping Sweep: □

Enable DNS Collection: □

Network blocks (one per line):

NetRelay Configuration

NetFlow

Enable NetFlow Agent: □

Internal Network blocks (one per line):

Forwarder Configuration

IP address:

Connection: Connect to: London-CAS1-fw (127.0.0.1:31415)

At this juncture, each of the component modules that are needed on the NAC Profiler Collector being added to the system configuration should be configured with the desired operating parameters. Again, not all the collector modules listed in Figure 7-1 will be configured/used on every NAC Profiler Collector. The form presented in the interface after the new Collector is added enables the configuration of the desired component modules that will be utilized on the new Collector.

For each of the component modules required on the NAC Profiler Collector, complete the procedures outlined below to configure/enable it. Execute an Apply Changes – Update Modules to save changes.

Changes made to Cisco NAC Profiler configuration are saved to the running configuration by clicking the Update Modules button on the Apply Changes page. The Apply Changes page is accessed by selecting the Apply Changes from the global navigation pane in the left hand margin on all pages of the Configuration Tab, or by selecting Apply Changes from the table on the main Configuration page.

Configuring a NetMap Collector Module

NetMap is the component of the NAC Profiler Collector that provides the network topology mapping engine. It communicates via SNMP with network devices added to the system configuration (see Chapter 8, “Adding Network Devices to the NAC Profiler Configuration”) at regular intervals as specified in the NAC Profiler Server module configuration (see Chapter 6, “NAC Profiler Server Configuration”). The NetMap component module collects information about the network topology and endpoint landscape to construct a model of the network used in the Endpoint Profiling process by Cisco NAC Profiler.

The NetMap component module is enabled on all NAC Profiler Collectors and in the majority of cases requires no additional configuration. Upon adding network devices to the configuration (see Chapter 8, “Adding Network Devices to the NAC Profiler Configuration”), the NetMap module will begin regular polling of the network devices assigned to it when the device is added to the configuration immediately after an Apply Changes is executed.

Note The Apply Changes page of the management interface includes a second button named ‘Re-Map.’ The Re-Map button causes the system to force all NetMap modules to query the assigned network devices for SNMP information and refresh the network model without restarting the NAC Profiler System.

NetMap uses SNMP Get, GetNext and GetBulk (when available) requests to query the SNMP agents running on the network infrastructure devices to gather specific Management Information Base (MIB) objects about their status based on device type (Layer 2 or Layer 3). By default, NetMap queries Layer 2 devices every 60 minutes and Layer 3 devices every 10 minutes.

The information gathered by the NetMap component module is augmented by the NetTrap component module which processes SNMP traps from edge devices to track the movement of endpoints in near real time. Configuration of NetTrap is covered later in this section. Upon receipt of a link state or new-MAC notification trap from a network device, the NetMap component module assigned to poll that device will initiate a poll to determine the change to the endpoint topology that resulting in the trap being sent by the network device.

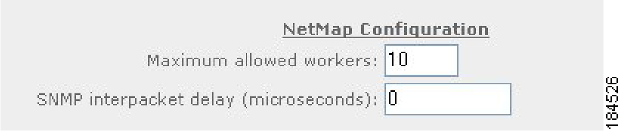
Editing a NetMap Collector Module

As a NAC Profiler Collector is added to the system configuration as described above use the following procedure to change any of the configurable parameters of the NetMap component module running on that Collector.

In most cases the default values of these parameters are sufficient, and no additional configuration is required.

Immediately after adding a NAC Profiler Collector to the system configuration, the NetMap section of the Edit Collector form appears as shown in Figure 7-4.

Figure 7-4 NetMap Configuration Section for the Edit Collector Form



NetMap Configuration

Maximum allowed workers: 10

SNMP interpacket delay (microseconds): 0

Each of the configurable parameters of NetMap is described below.

Maximum allowed workers

The NetMap component module on a Collector can fork multiple NetMap workers to poll network devices in parallel. This number sets the maximum number, therefore limiting the amount of SNMP traffic generated by NetMap. This value may be configured to allow up to 128 workers to be spawned at once, with the default value being 10.

SNMP inter-packet delay

This value represents the milliseconds delay between SNMP packets issued by NetMap and should not be altered unless the system is experiencing SNMP packet loss. The default value is 0.

After completing the NetMap module configuration, configure the other component modules (if required) as outlined below. If no other component modules require configuration, skip to Saving Edits to a Collector Configuration, page 7-15.

Configuring a NetTrap Collector Module

NetTrap is the component module running on each NAC Profiler Collector responsible for receiving and processing SNMP traps from the edge network devices being polled by the NetMap module running on the NAC Profiler Collector. The Endpoint Profiler system utilizes SNMP traps from the edge infrastructure when available in conjunction with NetMap to maintain an accurate model of the network. As described in Chapter 3, "Preparing for Deployment," whenever possible the edge infrastructure equipment should be configured to send Link State and New MAC Traps to the NAC Profiler Collector (management interface) running the NetMap module designated for polling via SNMP. As described in Chapter 8, "Adding Network Devices to the NAC Profiler Configuration," each network device added to Cisco NAC Profiler configuration is assigned to be polled by one of the NetMap components running on one of the Collectors to distribute SNMP polling. Each network device should send link state and or new MAC notification traps to the Collector running the NetMap component assigned to poll it. This requires a configuration change to the edge devices to include this IP address as a trap receiver, preferably for only the Link State and new MAC traps when available.

Before configuring infrastructure devices to send SNMP traps to Cisco NAC Profiler, it is advisable that the network administrator understand the volume and validity of the traps to be sent to Cisco NAC Profiler. Edge infrastructure equipment that sends excessive and/or erroneous trap information can cause the appliances running the NetTrap collector to consume excessive system resources and potentially impact performance and stability. Whenever possible, selectively configure traps on the edge devices to send only link state and new MAC traps to the NetTrap collector module.

Note While most SNMP-capable devices can be configured to send link state traps, MAC address change notification traps are vendor-specific and therefore may not be supported on all devices.

Note If the edge infrastructure devices are not configured to send SNMP Traps to Cisco NAC Profiler, there will be a delay in notification that a new end node has joined the network. New endpoints joining the network will not be discovered until the NetMap module polls the network device providing connectivity at the next scheduled poll.

Editing a NetTrap Collector Module

As the Edit Collector form indicates (see below), there are no configurable parameters for the NetTrap collector module. As a Collector is added to the system configuration, the NetTrap module is added and enabled automatically.

Figure 7-5 NetTrap Configuration Section of the Edit Collector Form

NetTrap Configuration
No configuration required

If no other component modules require configuration, skip to the "Saving Edits to a Collector Configuration" section on page 7-15.

Configuring a NetWatch Collector Module

NetWatch is the network packet analysis component module on NAC Profiler Collectors. A NetWatch module running on a NAC Collector can monitor one or more of the specified physical network interfaces on the CAS appliance for endpoint traffic useful for endpoint profiling and behavior monitoring. Typically, these physical interfaces are connected to network ports configured as SPAN/RSPAN ports providing visibility to endpoint traffic of interest redirected to the NetWatch component for the purposes of Endpoint Profiling and Behavior Monitoring.

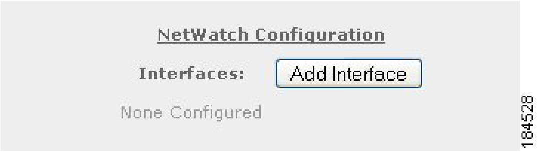
Note The NetWatch module must be configured to monitor traffic on one or more of the CAS interfaces (typically eth0 and or eth3) in order to enable the passive traffic analysis features of the NAC Profiler Collector being added to the system. Utilize the Edit NetWatch Module process outlined below to add one or more monitoring interfaces to the NetWatch module configuration upon adding a Collector to the system configuration.

Editing a NetWatch Module on a NAC Profiler Collector

As a NAC Profiler Collector is added to the system configuration as described above use the following procedure to change any of the configurable parameters of the NetWatch module running on that Collector.

Immediately after adding a NAC Profiler Collector to the system configuration, the NetWatch section of the Edit Collector form appears as shown in Figure 7-6.

Figure 7-6 NetWatch Configuration Section of Edit Collector Form



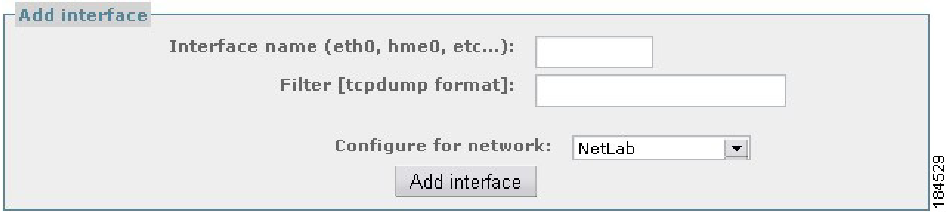
None Configured

As outlined in the last section, the newly added Collector will not have any physical interfaces on the appliance designated for passive monitoring. In order to enable the NetWatch module on this Collector, one or more physical addresses must be added to the NetWatch configuration for this collector. Follow the following procedures for adding, editing or deleting an interface to-from the NetWatch configuration on a Collector:

1. Adding Monitoring interfaces to a NetWatch module configuration:

   Select the Add Interface button in the NetWatch Configuration section of the Edit Collector to launch the NetWatch Add Interface form shown below:

Figure 7-7 Add NetWatch Interface Form



Configure for network: NetLab

Interface name

Specify an Ethernet interface name of the NAC Profiler Collector appliance that the NetWatch module is running on to be added as a monitoring interface. The two interfaces used typically are the management interface (eth0) and the eth3 interface. The eth3 interface is typically connected to a port configured for SPAN to redirect traffic of interest to the NetWatch component module for traffic analysis.

Adding the Management interface (eth0) to the NetWatch module running on the Collector avails all traffic received on that interface to NetWatch for passive analysis.

Filter name

The filter option is used when it is desirable to filter unwanted traffic from the NetWatch collection on the interface. When the amount of traffic on a monitoring interface is high, filters can be used to discard traffic not useful for Endpoint Profiling and or Behavior Monitoring to avoid using system resources on the CAS appliance unnecessarily.

The format of this field should be a tcpdump/libcap style string. For example:

```
net 128.16
dest net 128.16
tcp src port 443
```

For more examples please refer to the “Allowable primitives are:” section of the tcpdump man page website:

```
http://www.tcpdump.org/tcpdump_man.html
```

Configure for network

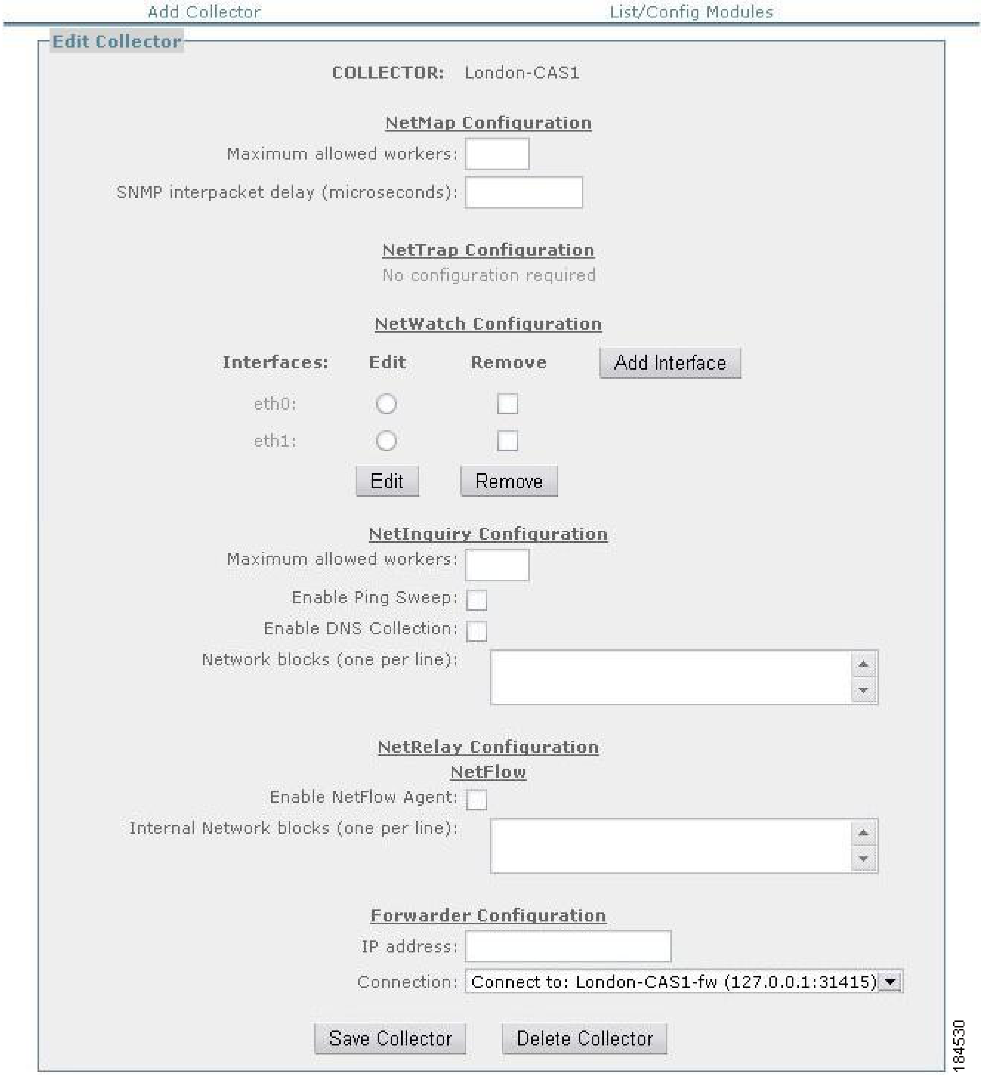
This parameter allows the specification of which of the host network address space(s) specified and named in the MyNetworks configuration (see Chapter 5, "Configuring NAC Profiler for the Target Environment") this monitoring interface will gather. The drop-down list is populated with the names of all networks saved in MyNetworks in the system configuration. If there are multiple networks defined, select the network name the interface being added to NetWatch should monitor.

Select the Add interface button to save the configured interface and return to the Edit Collector form. Adding additional interfaces to the NetWatch module configuration can be accomplished by repeating the process outlined above.

2. Editing/Removing interfaces from a NetWatch module configuration:

If monitoring interfaces have been added to the NetWatch component module configuration previously, the interface (or interfaces) will be listed, with an Edit radio button, and Remove checkbox to the right of each interface, as shown below.

Figure 7-8 Edit NetWatch Modules with Interfaces



Add Collector   List/Config Modules

Edit Collector

COLLECTOR: London-CAS1

NetMap Configuration

Maximum allowed workers:

SNMP interpacket delay (microseconds):

NetTrap Configuration

No configuration required

NetWatch Configuration

Interfaces:	Edit	Remove	Add Interface
eth0:	○	□	
eth1:	○	□	
	Edit	Remove	

NetInquiry Configuration

Maximum allowed workers:

Enable Ping Sweep: □

Enable DNS Collection: □

Network blocks (one per line):

NetRelay Configuration

NetFlow

Enable NetFlow Agent: □

Internal Network blocks (one per line):

Forwarder Configuration

IP address:

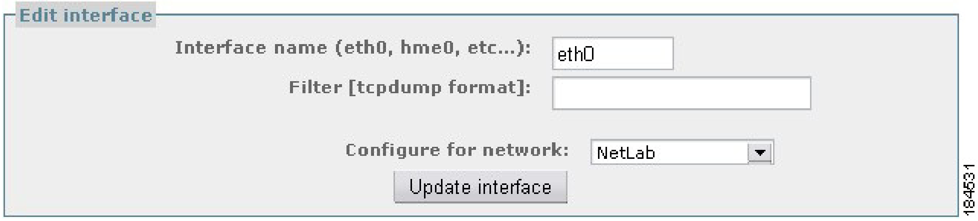
Connection: Connect to: London-CAS1-fw (127.0.0.1:31415)

Save Collector   Delete Collector

To remove an interface from a NetWatch configuration, select the Remove checkbox adjacent to the interface(s) to be removed and select the Remove button.

To edit an interface in a NetWatch configuration, select the Edit radio-button adjacent to the interface name, then select the Edit button below the interface radio button(s). This brings up the Edit interface form which reflects the current saved parameters for the interface as shown in the example below.

Figure 7-9 Edit NetWatch Interface



Edit interface

Interface name (eth0, hme0, etc...): eth0

Filter [tcpdump format]:

Configure for network: NetLab

The editable NetWatch interface parameters are:

Interface name

Specify an Ethernet interface name of the NAC Profiler Collector appliance that the NetWatch module is running on to be added as a monitoring interface. The two interfaces used typically are the management interface (eth0) and the eth3 interface. The eth3 interface is typically connected to a port configured for SPAN to redirect traffic of interest to the NetWatch collector module for traffic analysis.

Adding the Management interface (eth0) to the NetWatch module running on the Collector avails all traffic received on that interface.

Filter name

The filter option is used when it is desirable to filter unwanted traffic from the NetWatch collection on the interface. When the amount of traffic on a monitoring interface is high, filters can be used to discard traffic not useful for Endpoint Profiling and or Behavior Monitoring to avoid using system resources unnecessarily.

The format of this field should be a tcpdump/libcap style string. For example:

```
net 128.16
dest net 128.16
tcp src port 443
```

For more examples please refer to the “Allowable primitives are:” section of the tcpdump man page website:

http://www.tcpdump.org/tcpdump_man.html

Configure for network

This parameter allows the specification of which of the host network address space(s) specified and named in the MyNetworks configuration (see Chapter 5, “Configuring NAC Profiler for the Target Environment”) this interface will gather. The drop-down list is populated with the names of all networks saved in MyNetworks in the system configuration. If there are multiple networks defined, select the network name the interface being added to NetWatch should monitor.

Select the Add interface button to save the configured interface and return to the Edit Collector form.

Adding, editing or removing additional interfaces to the NetWatch module configuration can be accomplished by repeating the processes outlined above.

After completing the NetWatch module configuration, configure the other component modules (if required) as outlined below. If no other component modules require configuration, skip to the section entitled "Saving Edits to a Collector Configuration" section on page 7-15.

Configuring a NetInquiry Collector Module

The NetInquiry module provides an active means of Profiling endpoints that are difficult to Profile passively. This may be desirable in environments where the NAC Profiler Collector is not able to directly observe traffic from endpoints of interest that can be used for Endpoint Profiling, or in the case of endpoints that do not regularly generate traffic on the network.

Unlike active scanners used primarily for endpoint vulnerability assessment, the NetInquiry module will attempt to initiate communications with endpoints according to narrowly defined criteria (e.g., on a single TCP/UDP port), not broadly defined scans which can potentially harm some endpoints. The NetInquiry collector module operates in conjunction with designated TCP Open Port rules, and some Application rule types that can be used in the definition of Endpoint Profiles. Configuration of these rules is explained in detail in Chapter 9, "Configuring Endpoint Profiles."

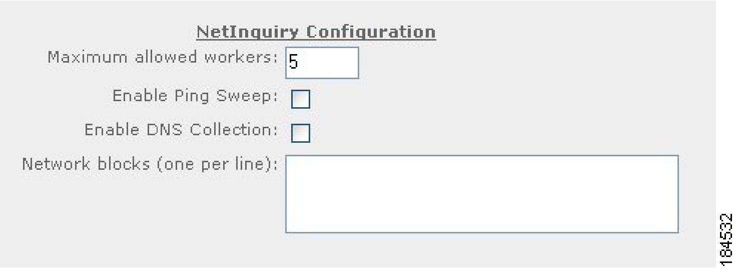
An additional control on this functionality is implemented within NAC Profiler which limits the scanning only to a specified number of devices. As outlined later in this section, the NetInquiry functionality is constrained to only the network blocks specified in the configuration of each NetInquiry module. The NetInquiry module initiates an attempt to actively probe the devices only on the specified subnets via the management interface of the NAC Profiler Collector appliance on which it is running. In this approach to active profiling, traffic that is extremely useful for the Endpoint Profiling process can be generated resulting in the receipt of traffic on the management interface of the appliance. That traffic is then available for analysis by the Profiler, and it is generated efficiently and with minimum impact on the endpoints or the network.

Editing a NetInquiry Collector Module

As a NAC Profiler Collector is added to the system configuration as described above use the following procedure to change any of the configurable parameters of the NetInquiry module running on that Collector.

Immediately after adding a NAC Profiler Collector to the system configuration, the NetInquiry section of the Edit Collector form appears as shown in Figure 7-10.

Figure 7-10 NetInquiry Configuration Section of the Edit Collector Form



NetInquiry Configuration

Maximum allowed workers: 5

Enable Ping Sweep: □

Enable DNS Collection: □

Network blocks (one per line):

Each of the configurable parameters of NetInquiry is described below.

Maximum allowed workers

The NetInquiry process can fork multiple NetInquiry workers to act in parallel. This number sets the maximum number, thereby limiting the amount of network traffic generated and the system resources used by NetInquiry. This value may be configured to allow up to 16 workers to be spawned at once, with the default value being 5.

Enable Ping Sweep

Selecting this option configures the NetInquiry module to ping the host addresses on the subnet(s) specified in the Network blocks field to determine whether or not they are presently active.

Enable DNS Collection

This optional feature of the NetInquiry collector modules enables Cisco NAC Profiler to perform name lookups on the addresses specified in the Network blocks field. The actively discovered name can then be used by the system to match DNS Name Application rules bound to endpoint Profiles.

Note This feature should only be used when DNS Name Application Rules are being used in enabled Endpoint Profiles. Cisco NAC Profiler will query the DNS for each host address on the subnet(s) specified in the Network Blocks parameter of the NetInquiry configuration when this parameter is checked in the NetInquiry module configuration.

Network Blocks

This field is used to specify the subnet or subnets which contain the endpoints that are desired to be actively probed by this NetInquiry collector module. The format is X.X.X.X/CIDR, for example 10.10.0.0/16 means any IP Address in which the first two octets are 10.

Add the subnet(s) that contain the hosts to be probed by NetInquiry, one per line.

After completing the NetInquiry module configuration, configure the other component modules (if required) as outlined below. If no other component modules require configuration, skip to the section entitled ***Saving Edits to a Collector Configuration*** later in this chapter.

Configuring a NetRelay Collector Module

The NetRelay collector module is an optional module that enables Cisco NAC Profiler to ingest captured data from other data collection systems. NetRelay can be especially useful for performing Endpoint Profiling on remote segments of the network (e.g., remote offices, etc.) that Cisco NAC Profiler cannot monitor directly. In order to utilize the NetRelay module in a NAC Profiler system, IP traffic data collectors such as NetFlow must already be in place on the network and collecting Netflow data on the endpoints of interest. The NetRelay collector module enables NAC Profiler to re-use this data for the purposes of Endpoint Profiling and Behavior Monitoring.

Netflow data is used by Cisco NAC Profiler in conjunction with Traffic rules which are described in Chapter 9, "Configuring Endpoint Profiles." Netflow data can be used in lieu of raw network traffic to enable Cisco NAC Profiler to examine traffic flows between endpoints for behavior specified in Traffic Rules bound to endpoint profiles.

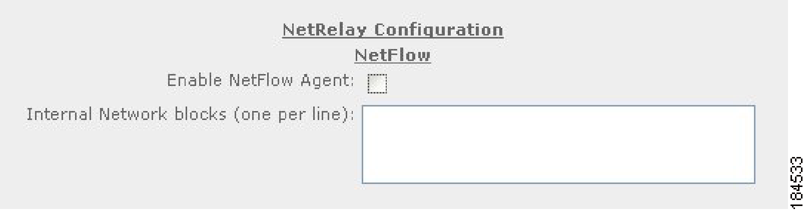
This functionality is dependent upon the presence of Netflow collector devices (e.g., routers, switches or other devices that have a Netflow collector capability) on the network segments of interest, with Netflow collection enabled and configured to forward their data to Cisco NAC Profiler.

Editing a NetRelay Collector Module

As a NAC Profiler Collector is added to the system configuration as described above use the following procedure to change any of the configurable parameters of the NetRelay module running on that Collector.

Immediately after adding a NAC Profiler Collector to the system configuration, the NetRelay section of the Edit Collector form appears as shown in Figure 7-11.

Figure 7-11 Table of Modules



NetRelay Configuration

NetFlow

Enable NetFlow Agent: □

Internal Network blocks (one per line):

Each of the configurable parameters of the NetRelay component is described below.

Enable NetFlow Agent

This option must be enabled in order for the NAC Profiler to accept Netflow traffic from Netflow collectors on the network configured to forward their data to Cisco NAC Profiler.

Internal Network Blocks

This field is used to specify the subnet or subnets which contain the host addresses that this NetRelay module should ingest Netflow data for. This should be limited to the IP host addresses of endpoints being Profiled via NetFlow.

The format is X.X.X.X/CIDR, for example 10.10.0.0/16 means any IP Address in which the first two octets are 10.

Add the subnet(s) that contain the host addresses NetRelay should ingest Netflow data for from the Netflow records it receives.

Saving Edits to a Collector Configuration

When all desired changes have been made to the NAC Profiler Collector configuration, select the Save Collector button to save all changes to the Collector.

Note Changes made to Collectors are saved to the running NAC Profiler system configuration by clicking the Update Modules button on the Apply Changes page. The Apply Changes page is accessed by selecting the Apply Changes from the global navigation pane in the left hand margin on all pages of the Configuration Tab, or by selecting Apply Changes from the table on the main Configuration page.

Determining Status of NAC Profiler Collectors

After saving the edits to a Collector, the status of all Collectors in Cisco NAC Profiler as well as the Server can be quickly ascertained by navigating to the Configuration tab, selecting Profiler Modules from the table in the main pane or from the left-hand navigation pane, then selecting List Profiler Modules. An example Table of Collectors showing Collector status is shown below:

Figure 7-12 List/Config Modules

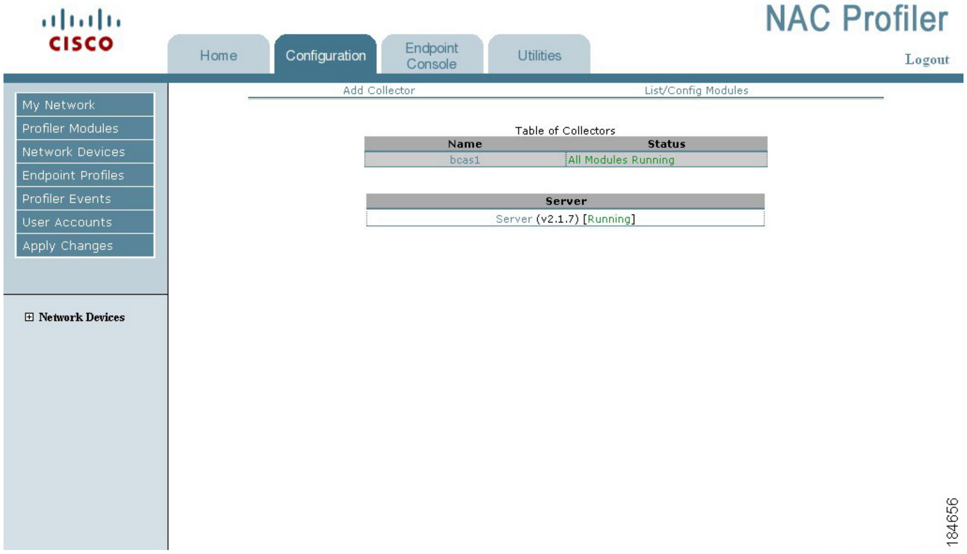


Table of Collectors

Name	Status
bcas1	All Modules Running

Server
Server (v2.1.7) [Running]

The Status column of the Table of Collectors indicates the condition of the underlying Forwarder and the component modules of each Collector in Cisco NAC Profiler configuration. There are seven possible Collector statuses that can be reported in the Table of Modules. Table 7-3 describes Collector Status messages.

Table 7-3 Collector Status Messages

Status	Interpretation
All Modules Running	All modules of the Collector have been contacted by the Server and are running. The Collector is online and operating normally.
All Modules Stopped	All modules of the Collector have been contacted by the Server, but they are in a stopped condition. This is typically a transitory condition resulting from the system restart following an Apply Changes.
One or More Modules Stopped	All modules of the Collector have been contacted by the Server, but one or more are in a stopped condition. Again, this may be a transitory state as some modules may take longer to come back online after a system restart. If the condition does not clear, follow the procedures outlined in Troubleshooting Component Modules on a Collector, page 7-17 to determine what module(s) are in the stopped condition.

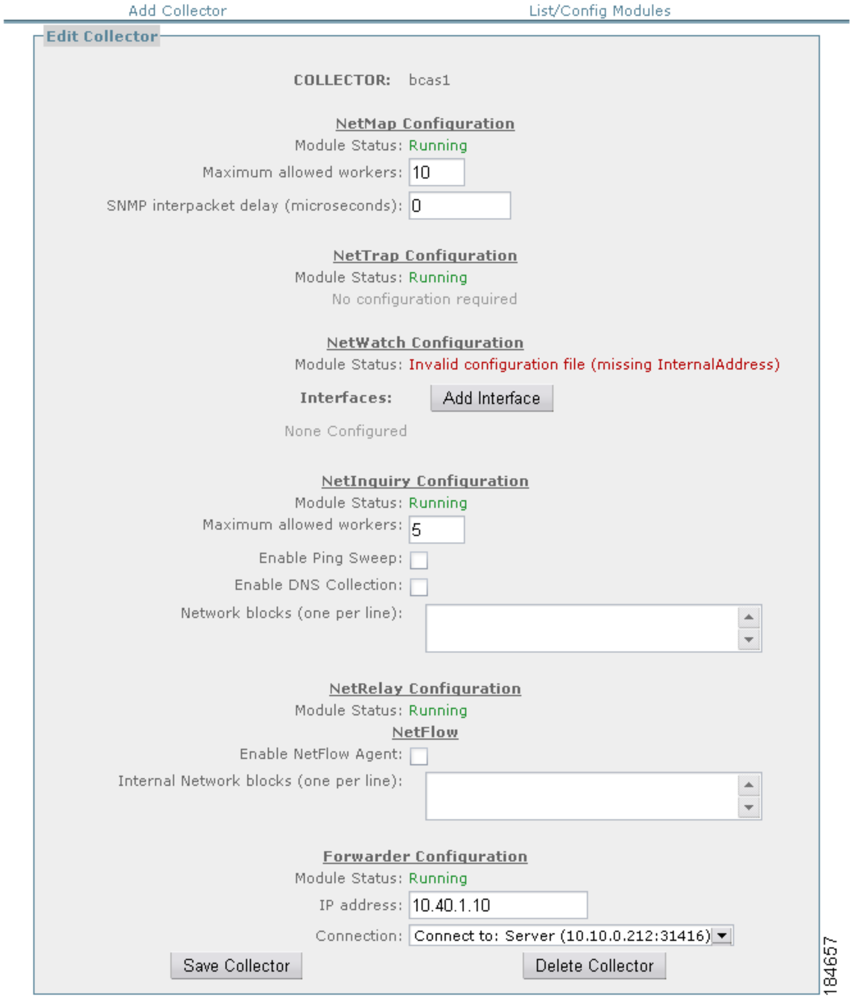
Table 7-3 Collector Status Messages

Status	Interpretation
Not Contacted	The NAC Profiler Server is unable to establish communications with the Forwarder module running on the NAC Profiler Collector. Status of the Collector and its component modules cannot be determined by the Server. See Troubleshooting Component Modules on a Collector, page 7-17.
Licensing Issue	Either no license is installed for the Collector or the installed license is invalid. Upload a valid license key file from the Home tab. See Chapter 5, "Configuring NAC Profiler for the Target Environment."
One or More Modules Restarting	One or more component modules on the Collector are in the process of restarting. This is a very short transitory state between stopped and running that is not normally observed. It occurs when a Collector initially establishes contact with the Server when a new system is brought online.
One or more Modules reporting an error	One or more component modules on the Collector have posted an error message. This typically indicates an error in the module configuration.

Troubleshooting Component Modules on a Collector

The Table of Collectors provides a top-level view of each NAC Profiler Collector in Cisco NAC Profiler. If the status of a Collector is other than "All Modules Running," status of the underlying modules of a given Collector can be determined by selecting the name of the Collector in the table of Collectors to open the Edit Collector form. See Figure 7-13.

Figure 7-13 Edit Collector Form Showing Different Module Statuses



COLLECTOR: bcas1

NetMap Configuration
Module Status: Running
Maximum allowed workers: 10
SNMP interpacket delay (microseconds): 0

NetTrap Configuration
Module Status: Running
No configuration required

NetWatch Configuration
Module Status: Invalid configuration file (missing InternalAddress)
Interfaces: Add Interface
None Configured

NetInquiry Configuration
Module Status: Running
Maximum allowed workers: 5
Enable Ping Sweep: □
Enable DNS Collection: □
Network blocks (one per line):

NetRelay Configuration
Module Status: Running
NetFlow
Enable NetFlow Agent: □
Internal Network blocks (one per line):

Forwarder Configuration
Module Status: Running
IP address: 10.40.1.10
Connection: Connect to: Server (10.10.0.212:31416)

As shown in Figure 7-13, each of the modules running on a Collector (e.g., NetMap, NetTrap, NetWatch, NetInquiry, NetRelay and Forwarder) has a Module Status indicated at the top of each section of the form pertaining to each component module on the Collector. The status of a component module can be one of the following:

- Running – the component module is running and reporting normal status.
- Stalled – When component modules on a Collector report a status of stalled this indicates that contact with the Collector was established but subsequently lost, typically due to the loss of network communications between the Server and Collector.
- Stopped – the component module is not running and is likely restarting.
- No contact – The Server has not made contact with the Collector or the component modules running on it and therefore cannot ascertain status. If the Collector status is indicating 'Not contacted' as described above, the component modules indicate 'no contact' individually.
- Invalid configuration file (missing Internal Address) – NetWatch–specific error condition that indicates that a monitoring interface was never specified for the NetWatch component module.

A Module Status of 'running' indicates that the module is running and requires no attention.

A Module Status of ‘stopped’ indicates that the Server is in communications with the Forwarder on Collector, but the respective component module was not running. After a system restart (following an Apply Changes -> Update Modules for example) some amount of time may be required for the underlying modules to restart using the new configuration sent down to the module by the Server (if applicable). Wait several minutes and check the status again by refreshing the page. If a module continues to indicate a status of stopped, further troubleshooting is required. The troubleshooting should begin with checking the existing configuration of the affected module to ensure it is configured according to the instructions in this chapter. After verifying the configuration an Apply Changes -> Update Modules should be performed to attempt restart of the module to return it to a running status. Regardless of whether or not configuration of the module is modified, an Apply Changes -> Update Modules is recommended as the first step in attempting to restart a stopped module on a NAC Profiler Collector.

When the status of a module indicates ‘no contact’, this indicates the Server and Forwarder being unable to establish communication over the network (e.g., collector status is ‘Not Contacted.’ The parameters for the communication between the Server and Collector are configured as described in Chapter 4, “Installation and Initial Configuration” (when a new NAC Profiler Collector is initially configured on a CAS appliance), in the NAC Profiler Server configuration as described in Chapter 6, “NAC Profiler Server Configuration.”, and in the Forwarder module configuration performed when adding the Collector to the configuration as described earlier in this chapter.

The parameters for the communication such as Collector name (must match hostname of the Collector/CAS), connection type (e.g., client or server), IP address, network connection defined on the Server, connection on the Forwarder, encryption type and shared secrets on both must be consistent in order for the communication between Server and Forwarder to be established. Revisit these parameters in the NAC Profiler Collector setup, the Server and Forwarder configuration to ensure that the configurations are consistent. In addition, verify that there are no other measures deployed (e.g., ACLs, firewalls, etc.) that would prevent TCP communications between the NAC Profiler Server and the NAC Profiler Collector paying particular attention in the case of a firewall deployed between the devices that traversal is possible on the selected port number. When these troubleshooting steps have been completed, perform the Apply Changes -> Update Modules procedure to restart all modules which will result in a reattempt to establish the network connection between the Server and Collector.

Component modules reporting a ‘stalled’ status is likely due to the Collector going offline completely or a condition in the network that has interrupted the TCP connection between the Collector and the Server. If the Collector is determined to be up and running, troubleshooting should begin with determining if the connection between the devices is established beginning with a ‘ping’ between devices to determine the status of network communications between the appliances.

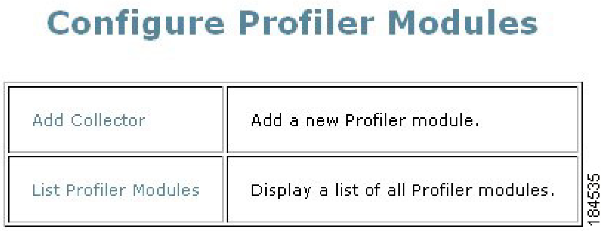
In the case of component modules reporting an error, in general this is due to an error in the configuration, or in the case of the NetWatch module specifically, not having a monitoring interface specified in the component module configuration. Verify the configuration of the component module to ensure at least one of the interfaces on the Collector appliance is specified as a monitoring interface.

Editing a NAC Profiler Collector Configuration

Once a Collector has been added to the system configuration, changes can be made to the configuration parameters of the Forwarder and collector modules running on the NAC Profiler Collector.

To edit a Collector previously saved to the NAC Profiler configuration, navigate to the Configuration tab and select Profiler Modules from the table in the main pane or from the left hand navigation pane to display the Configure Profiler Modules page shown in Figure 7-14.

Figure 7-14 Configure Profiler Modules Table



Configure Profiler Modules

Add Collector	Add a new Profiler module.
List Profiler Modules	Display a list of all Profiler modules.

Select List Profiler Modules from the table to display the Table of Collectors/Table of Servers page. An example of this page is shown in Figure 7-15.

Figure 7-15 List/Config Modules

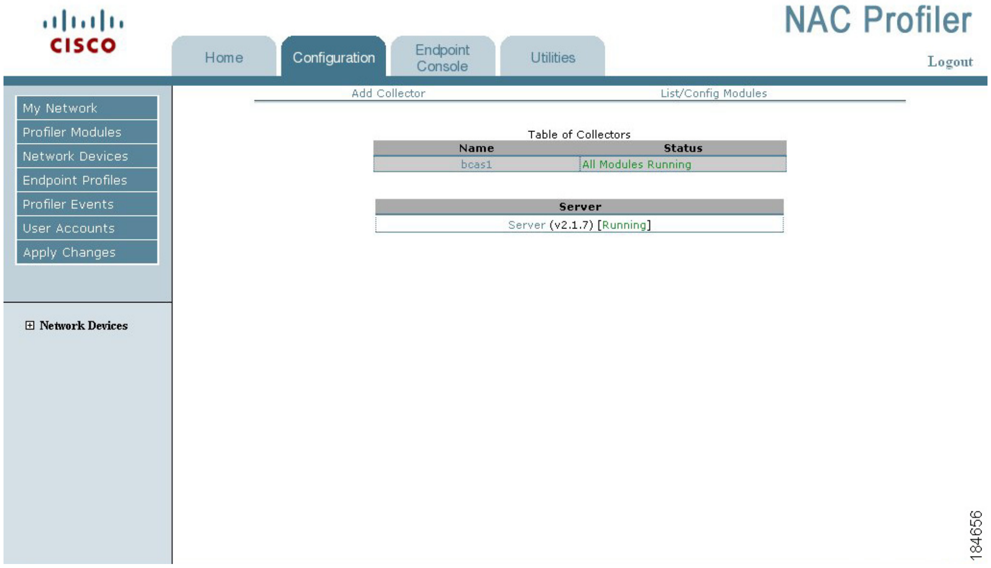


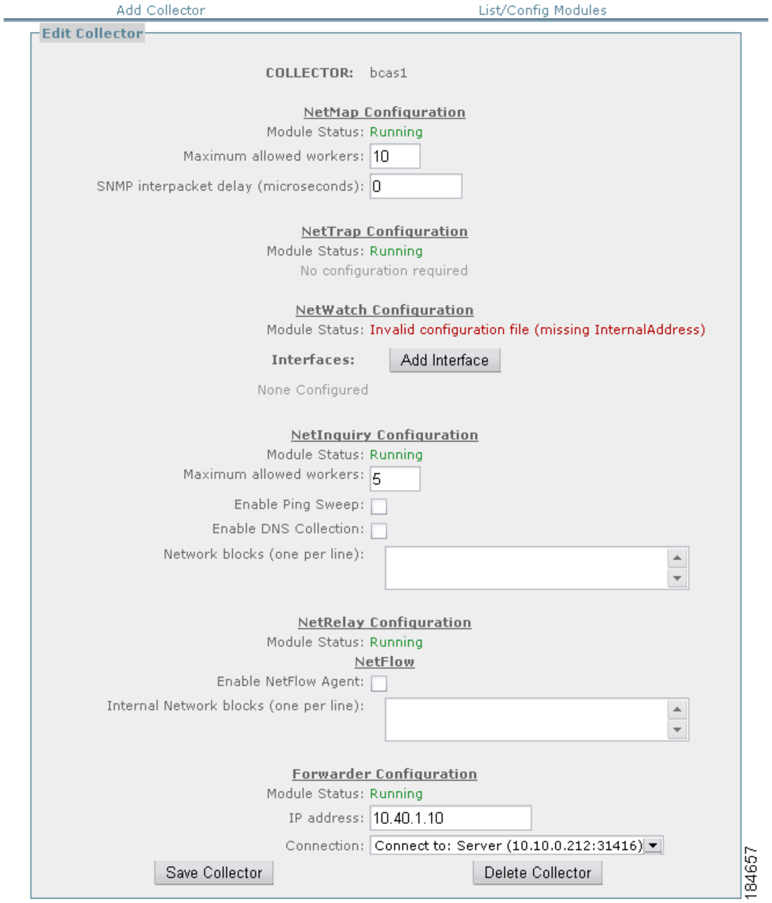
Table of Collectors

Name	Status
bcas1	All Modules Running

Server
Server (v2.1.7) [Running]

To edit a Collector, more specifically the configuration parameters of the component modules and or Forwarder of the Collector, select the Collector name from the table, which opens the Edit Collector form for the Collector already saved to the configuration. An example of the Edit Collector form for a running Collector module that has been contacted by the Server is shown in Figure 7-16.

Figure 7-16 Edit Collector Form



COLLECTOR: bcas1

NetMap Configuration
Module Status: Running
Maximum allowed workers: 10
SNMP interpacket delay (microseconds): 0

NetTrap Configuration
Module Status: Running
No configuration required

NetWatch Configuration
Module Status: Invalid configuration file (missing InternalAddress)
Interfaces:
None Configured

NetInquiry Configuration
Module Status: Running
Maximum allowed workers: 5
Enable Ping Sweep: □
Enable DNS Collection: □
Network blocks (one per line):

NetRelay Configuration
Module Status: Running
NetFlow
Enable NetFlow Agent: □
Internal Network blocks (one per line):

Forwarder Configuration
Module Status: Running
IP address: 10.40.1.10
Connection: Connect to: Server (10.10.0.212:31416)

This is the same page used to enter the initial configuration of the modules running on the collector, and described in detail in the beginning sections of this chapter. These sections outline in detail the configuration parameters of each of the component modules of a Cisco NAC Collector. The Edit Collector form for a contacted Collector indicates below each collector module name the status of each module as described in the previous section.

Refer to the earlier sections in this chapter which cover the configuration of each module of a Cisco NAC Collector to make desired changes. When all desired changes have been made to components of the Collector, select the Save Collector button at the bottom of the form to save configuration changes.

Changes made to Profiler Modules are saved to the running NAC Profiler system configuration by clicking the Update Modules button on the Apply Changes page. The Apply Changes page is accessed by selecting the Apply Changes from the global navigation pane in the left hand margin on all pages of the Configuration Tab, or by selecting Apply Changes from the table on the main Configuration page.

Delete a Collector from the System Configuration

To delete a Collector from the system configuration, navigate to the Table of Collectors, and select the name of the collector to be deleted. The Edit Collector form is displayed. Scroll down to the bottom of the form to the Delete Collector button. Selecting this button will delete the Collector configuration from the system configuration, and return the interface to the Table of Collector/Table of Servers page, displaying a message that the modules on the deleted Collector have been deleted from the database. The deleted Collector is removed from the table of Collectors. If desired, the Collector can be re-added to the system configuration using the procedure outlined earlier in this chapter.