CHAPTER 13

# Integrating with the Cisco NAC Appliance

This chapter contains the following topics:



## Overview

Cisco NAC Profiler can be tightly integrated with the Cisco NAC Appliance. The integration of Endpoint Profiling and Identity Monitoring with Cisco NAC Appliance provides several distinct advantages in the deployment and ongoing operation of Cisco NAC Appliance in enterprise networks. Cisco NAC Profiler can significantly decrease the administrative burden and greatly improve the secure and reliable handling of endpoint types that are unable to interact with Cisco NAC Appliance either automatically or via user input.

Examples of endpoints that are non-NAC compatible include printers, UPS, IP Phones, HVAC control systems – and a myriad of other endpoints that lack supported means to submit credentials when challenged by the admission control system, and/or lack a user to drive the process.

The Cisco NAC Appliance system has a built-in capability for handling non-NAC endpoints such as printers and other non-NAC compatible devices. The devices that cannot interact with Cisco NAC Appliance in the same way as user devices such as desktop and laptop computers can be identified and added to a table in the NAC Manager.

This table, accessible from the Device Management section of the NAC Manager is commonly referred to as the Device Filter List. The Device Filter List is populated with the list of endpoints (by MAC address) that are known to require special handling by the Cisco NAC Appliance system in order to be admitted onto the network.

Endpoints that have their MAC addresses added to the Device Filter list in the NAC Manager are handled by exception by the NAC system whenever these devices join the network. An endpoint with its MAC address on the Device Filter List is accorded options to bypass authentication and posture assessment. This enables endpoints that have inherent limitations in their ability to authenticate or have their posture assessed to be reliably and securely admitted to the NAC-enabled network.

If a Cisco NAC Profiler system is not deployed alongside Cisco NAC Appliance, the initial population and ongoing management of endpoint entries in the NAC Manager Device Filter List is performed manually by the Cisco NAC Appliance administrator. This process requires not only the identification of the endpoints by MAC address, it requires each of the non-NAC compatible devices be added to the device filter manually along with the desired admission policy.

The administrative burden and potential for errors in large enterprise environments resulting from manual management of the Device Filter List is high. The potential also exists for endpoint information in the Device Filter List to get stale as devices are retired or otherwise removed from the environment unless the list can be attended to on almost a daily basis.

Because the endpoints on the Device Filter list can be allowed access to the network for as long as their MAC address is on the list, and there is no built-in mechanism in the Cisco NAC Appliance solution to police the activities of these devices, the Cisco NAC Profiler solution mitigates the need for an ongoing and potentially intensive manual intervention that can be error prone.

The integration of Cisco NAC Profiler with Cisco NAC Appliance significantly enhances the ability to provide reliable and secure access to the NAC-enabled network while significantly decreasing administrative burden. Cisco NAC Profiler enables the automated discovery and identification of non-NAC compatible endpoints across the entire network environment in which Cisco NAC Appliance will be deployed in an automated, highly accurate and non-intrusive fashion.

Cisco NAC Profiler can be designed to segregate the non-NAC endpoints from the NAC endpoints such as desktop and laptop computers. The non-NAC endpoints can be added to the device filter list on the NAC Manager automatically, via the Cisco NAC Profiler integration with Cisco NAC Appliance, as endpoints are discovered and categorized into the Profiles that are created for all the non-NAC endpoints that may attempt to connect to the network through edge ports under NAC management.

Just as important, Cisco NAC Profiler has the ability to remove endpoints from the device filter list. This functionality is provided by the Identity Monitoring function of Cisco NAC Profiler which constantly evaluates endpoint data looking for changes indicative of changes in endpoint identity. Cisco NAC Profiler is constantly monitoring the observable attributes of endpoint identity such as the application-specific network traffic being generated by the endpoint or markers of specific operating systems.

When observations indicate new or inconsistent attributes that warrants a change in Profile, Cisco NAC Profiler will re-categorize the endpoint to the new Profile. If the new Profile is one designed to compartmentalize NAC-capable endpoints, Cisco NAC Profiler will remove the associated MAC address from the Device Filter list of the NAC Manager. As an option, upon that change Cisco NAC Profiler can signal the NAC Manager to force the endpoint to re-authenticate via the Custom API functionality described later in the chapter.

As the entry is removed from the Filter List, any network access privileges that were assigned are revoked as the endpoint attempts to re-authenticate. For that endpoint to regain network access, it must undergo the full NAC authentication and posturing prescribed for NAC-capable endpoints as it is no longer permitted access by MAC authentication. Essentially this functionality provided by Cisco NAC Profiler adds to the Cisco NAC Appliance solution an additional credential beyond MAC address for endpoints on the Device Filter list, a credential that can be best described as endpoint identity verification.

This is particularly effective in combating the “MAC spoofing” scenario when a general purpose endpoint (for example, laptop or desk top computer) is configured to use the MAC address of a special-purpose endpoint known to have MAC authentication privileges. Because Cisco NAC Profiler is constantly monitoring the identity attributes of each endpoint on the device filter list, ensuring that the current attributes are consistent with previously observed attributes that had led to the endpoint being allowed onto the network without full NAC authentication and posturing.

In addition, when the Database Maintenance option for Endpoint Timeout are enabled, Cisco NAC Profiler also monitors each discovered endpoint for activity on the network, tracking the time of refresh of endpoint profiling data collected. Endpoints that have been removed from the network, indicated no refresh of endpoint profiling data from the Collectors for a configurable number of days can be used to effect the removal of retired endpoints from the Device Filter list.

In this manner, Cisco NAC Profiler is able to continually prune the Device Filter List of the entries for endpoints that are no longer in use automating this aspect of administration of the Cisco NAC Appliance system over its entire lifecycle.

In summary, integration of Cisco NAC Profiler system with Cisco NAC Appliance can result in a highly effective NAC system for all endpoints on the network: both those that can interact with Cisco NAC Appliance, and those that cannot. Cisco NAC Profiler significantly reduces the administrative burden required for handling non-NAC compatible endpoints while providing continuous monitoring of the identity of endpoints, ensuring consistency with network policy.

# Cisco NAC Appliance Integration

The underlying mechanism of the integration of Cisco NAC Profiler with Cisco NAC Appliance is the NAC Profiler Server's ability to provision (for example, add or remove) entries on the NAC Manager Device Filter list so that endpoints in selected Profiles in the NAC Profiler database are maintained in synch with those on the Filter List. Cisco NAC Profiler provisions the NAC Manager Filter List via two methods:

1. By making calls directly to the NAC Appliance API allowing Cisco NAC Profiler to add/remove entries on the Filter List.

2. Via SQL calls over SSH in order to compare current NAC Manager Device Filter list entries against the Profiler database, and make updates accordingly.

This second method is referred to henceforth as "full synchronization," and after configuration of the NAC Appliance integration as described in the next section will be performed by the integration layer in the following cases:

- When the NAC Profiler system is restarted through the execution of Apply Changes -> Update Modules, or Apply Changes -> Re-model
- Every one hour during steady-state NAC Profiler system operation.

During steady-state operation, as changes occur in the NAC Profiler endpoint database--specifically as endpoints are profiled into or out of profiles matching the enabled Cisco NAC Events configured on NAC Profiler--Device Filter list entries on the NAC Manager are added or removed via the API calls as the changes occur. This synchronization functionality is referred to as "event handler" mode.

In addition, if the Custom API option is enabled, Cisco NAC Profiler may also request that the NAC Manager bounce the switch port connecting the device as endpoints are added or leave profiles matching enabled NAC events. See, Configuration of Profile Rules in the Application Rule Family, page 10-5.

This mechanism enables the immediate re-authentication of new endpoints that join the network and are subsequently profiled by Cisco NAC Profiler into a profile that is enabled for admission onto the network without full NAC authentication and posturing. This enables automated handling of the addition of new, non-NAC compatible endpoints to the network.

Conversely, if an endpoint is re-profiled and removed from the NAC Manager Device Filter list it is typically because the identity attributes of the endpoint have changed. The endpoint is now exhibiting attributes that are indicative that it may no longer be a non-NAC compatible endpoint.

In this case the re-authentication prompted by the change in profile and resulting port bounce cause the endpoint to be removed from the network. This is the case of detection and handling of the MAC spoofing scenario by the Cisco NAC Profiler integration with the Cisco NAC Manager.

When creating or updating an entry on the NAC Manager Device Filter list, Cisco NAC Profiler may manipulate any of the following attributes of the filter list entry for a given MAC address:

- Description field. Cisco NAC Profiler will populate the description field of entries it makes on the Device Filter list with the Cisco NAC Profiler Profile name and a link to the MAC Endpoint Summary data for the endpoint.
- Access Type, and Role for Access Types of “Use Role” and “Check.”

# Configuring Cisco NAC Appliance Integration

Configuration of the integration of Cisco NAC Profiler and Cisco NAC Appliance consists of four distinct steps or tasks that must be followed in order.

**Step 1** Configuration of the NAC Profiler Server with the information required for it to communicate with the NAC Manager via the Cisco NAC Appliance API. See Cisco NAC Profiler Server Configuration, page 13-4.

**Step 2** Establish SSH key-based authentication for the purposes of the NAC Profiler Server-NAC Manager synchronization functionality briefly described in the last section. The setup is performed by a command line operation run on the NAC Profiler Server, or Primary appliance of a NAC Profiler HA-pair. See Configure SSH Key-Based Authentication, page 13-8.

**Step 3** Configure a special NAC Profiler event type, called a “NAC Event.” NAC Events are special-purpose Profile Change Events as described in Chapter 12, “Configuring Cisco NAC Profiler Events.” NAC Events define the logic for the system in making decisions to add or remove MAC addresses from the Device Filter list on the NAC Manager via the aforementioned methods. See Creating NAC Events, page 13-10

**Step 4** Perform an initial full synchronization to synchronize the NAC Profiler database and NAC Appliance NAC Manager. When the full synchronization is performed, NAC Profiler will determine all endpoints in the Profiles designated for provisioning to the NAC Manager by processing the enabled Cisco NAC events, and create entries for each endpoint on the NAC Manager Device Filter List. See Synchronizing Cisco NAC Profiler and the NAC Manager Device Filter List, page 13-13.

# Cisco NAC Profiler Server Configuration

The primary task in this workflow consists of providing the NAC Profiler Server with the necessary information about the NAC Manager in the Cisco NAC Appliance system to enable communications between Cisco NAC Profiler and the NAC Manager via the API.

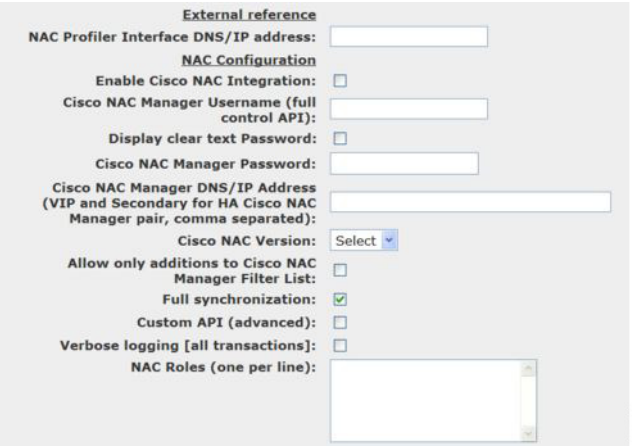
These parameters also provide the SSH key-based authentication setup script run in the next step with the information it needs to complete that process. Prior to beginning this step, collect the necessary information about the Cisco NAC Appliance configuration such as:

- The DNS Name or IP address of the NAC Manager. (For NAC Manager HA pairs, the NAC Manager HA-pair service (VIP) DNS name or IP address and the DNS Name/IP address of the NAC Manager HA-pair secondary node at the time of configuration must be entered so that keyless SSH is properly setup between the Profiler and **both** members of the NAC Manager pair in the next step.

  This allows the NAC Profiler to perform the full synchronization to the NAC Manager regardless of which appliance is the Primary node at any point in time).
- NAC Manager administrator username and password for a NAC Manager web UI user with Full Control API Access Control Policy.
- NAC version.
- Any NAC Roles that might be assigned to non-NAC endpoints provisioned by Cisco NAC Profiler to the NAC Manager Device Filter list, applicable only for adding Device Filter entries with the Role or Check Access Type.
- The DNS domain-name of the NAC Profiler Server, VIP for HA-pairs (alternatively, the IP address of the NAC Profiler Server (or VIP for HA pair) may be substituted, but this is not recommended).

To configure the required Profiler Server parameters for integration with a Cisco NAC Appliance, go to the Home Tab, then select the Server module link in the Profiler Modules table to bring up the Configure Server form. Scroll down the form to the parameter entitled "External reference," which is placed immediately above the Cisco NAC Configuration parameters. Figure 13-1 shows the Cisco NAC Appliance integration-specific parameters of the Configure Server form prior to the entry of any parameters for the environment.

***Figure 13-1 Profiler Server Module Parameters for Profiler Integration with Cisco NAC Appliance***




The following paragraphs outline the purpose of each of these parameters and guide completion of this part of the configuration.

**Tip** The Full Synchronization option is checked (on) by default on all systems. This parameter must be checked for the integration feature to operate correctly, and should be verified during configuration of the integration feature.

**Step 1** Enter the NAC Profiler Server External Reference.

Enter the DNS domain-name (preferred) or IP address of the management interface of the NAC Profiler Server. The DNS domain-name or IP address entered here will be used for the web link that will be embedded in the description field of each entry that NAC Profiler creates in the NAC Manager Device Filter list.

These web links give the administrator the ability to easily refer to Cisco NAC Profiler to find out more details about endpoints entered into the Device Filter List directly from the NAC Manager interface. In implementations where the NAC Profiler Server is an HA-pair, the HA-pair VIP/service DNS domain-name or IP address should be entered for this parameter.

**Step 2** Enable Cisco NAC Integration.

This check box **must** be selected in order to enable the NAC integration layer on the NAC Profiler system.

**Step 3** Enter a valid NAC Manager Web UI Username.

Enter a valid Administrator user name that has been configured on the NAC Manager server. NAC Profiler will use this name to gain administrator-level access to the NAC Manager via the Cisco NAC Appliance API for the purpose of provisioning the Device Filter list.

**Note** An administrator user can be created on the NAC Manager specific to the Cisco NAC Profiler integration which has API-level administrative access only. Refer to the applicable *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* for instructions on how to create a NAC Manager administrator user with only API-level access. Note that the administrative user must be granted "full control" API access. Failure to configure Cisco NAC Profiler with valid NAC Manager user credentials with full control API access will prevent Cisco NAC Profiler from being able to provision endpoints to/from the Device Filter List on the NAC Manager.

**Step 4** Enter the Password for the NAC Manager Web UI User.

Enter the password assigned to the Admin user on the NAC Manager specified above to be used by Cisco NAC Profiler when accessing the Cisco NAC Appliance API.

**Note** To view the NAC Manager password entered in clear text, select the "Display clear text password "check box immediately above NAC Manager Password field. This will toggle the entered password between obscured (unchecked) and clear text (checked) so the entered password can be verified.

**Step 5** Enter the NAC Manager Address/DNS domain-name.

Enter the DNS domain-name of the NAC Manager this NAC Profiler Server will manage the Device Filter list for. Alternatively, if DNS is not set up for NAC Profiler or if a DNS address record has not been created for the NAC Manager, the IP address of the NAC Manager can be entered.

When the NAC Manager is deployed as an HA-pair, the NAC Profiler Server configuration needs to have the following comma-separated DNS domain-names or IP addresses:

- NAC Manager HA-pair service (VIP)
- NAC Manager HA-pair secondary node

**Note** The setup of the SSH key-based authentication which enables the synchronization function described earlier **must** be completed on both appliances in a NAC Manager HA-pair. Providing the NAC Manager HA-pair service (VIP) allows the setup of SSH key-based authentication on the current primary node of the NAC Manager pair. Providing the IP of the secondary node at the time of configuration allows the setup script to complete the SSH key-based authentication setup on that appliance as the integration configuration is performed. If the secondary node information is not provided, or is provided incorrectly, the synchronization between Cisco NAC Profiler and the Cisco NAC Manager cannot be performed should the NAC Manager pair fail over.

**Tip** Determination of the IP of the NAC Manager Secondary node can be determined from the NAC Manager User Interface. From the Administration Menu, select CCA Manager. Select the Failover tab, and the resulting page clearly displays the DNS name and IP address of the Secondary node's eth0 interface. Refer to the applicable *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* for instructions on how to determine DNS/address information for the nodes of an active NAC Manager pair.

**Step 6** Enter the NAC Appliance Version.

Select the version of the NAC Appliance system this NAC Profiler system is being integrated with from the drop-down menu.

**Step 7** **Optional** - Set Allow only additions to NAC Manager Filter List option as desired.

If selected, Cisco NAC Profiler will manage the Device Filter list on the NAC Manager in the following manner: Once an entry has been created on the Device Filter list by Cisco NAC Profiler, the Profiler will **not** delete the entry nor modify the Access Type attribute of the endpoint. Effectively, selecting this option disables the removal/modification of the Device Filter list entries made by Cisco NAC Profiler.

The Identity Monitoring function of Cisco NAC Profiler for all endpoints added to the Device Filter List of the NAC Manager will be disabled, and retired endpoints will not be removed as they are timed out via the Endpoint Timeout. As endpoints are profiled into endpoint profiles matching enabled NAC Events, they are added to the NAC Manager in accordance with the configuration of the NAC event, and will remain in the state indefinitely unless action is taken by the Administrator.

Note that although this option is selected, Cisco NAC Profiler can still make changes to the description field in the Filter List, in particular changing the NAC Event Name recorded in the description of an endpoint should its profile change. This option changes the result of a change in Profile in that endpoints that transition do not have their access to the network revoked or modified due to a change in Profile.

**Step 8** Select Full Synchronization On (checked).

This parameter must be selected for normal operation of the synchronization function. Any time an Apply Changes -> Update Modules or, Apply Changes -> Re-model is executed via the Cisco NAC Profiler UI, a full synchronization between Cisco NAC Profiler and the Cisco NAC Manager will be executed as described in Synchronizing Cisco NAC Profiler and the NAC Manager Device Filter List, page 13-13.

**Step 9** Custom API, Check if desired.

Review the description and instructions for the configuration of this advanced option described in Use of "Custom API" Feature, page 11-18.

**Step 10** Enable Verbose Logging if desired.

Use this check box to enable verbose logging if desired. Enabling Verbose Logging results in all interactions with the Cisco NAC Appliance API to be logged (both normal operations and errors). By default, only errors are logged. Instruction for viewing these logs follows in a subsequent section.

**Step 11** Add NAC Roles as required.

This field is only required if network access to be provisioned to non-NAC endpoints provisioned to the Device Filter List will be differentiated via the Cisco NAC Appliance "User Role" construct. Each entry in the NAC Manager filter table has an "Access Type" attribute that specifies the type of network access to be applied for the given endpoint. If Cisco NAC Profiler is to add entries with Access Type of "Use Role" or "Check" then this field must be filled in to list all User Roles (one per line) configured on the Cisco NAC Appliance system that could be assigned to non-NAC endpoints provisioned to the Device Filter list via Cisco NAC Profiler. If Cisco NAC Profiler will only add entries with the "Ignore", "Allow" and "Deny" Access Types this field can be left blank.

Refer to the *Cisco NAC Appliance- Clean Access Manager Installation and Configuration Guide* for a discussion of Access Types and User Roles, as well as Creating NAC Events, page 13-10 for further details.

At the completion of these steps, the NAC Profiler Server module configuration for integration with Cisco NAC Appliance is complete. Be sure to select the Update Server button at the bottom of the form to save the changes to the configuration, then proceed with next task in the configuration of the integration, the configuration of SSH Key-Based Authentication between the Profiler Server and the NAC Manager.

# Configure SSH Key-Based Authentication

Complete this task to set up secure communications via key-based SSH between the NAC Profiler Server and the Cisco NAC Appliance NAC Manager (or NAC Manager HA-pair) used for the synchronization function. This requires the execution of a script via the command line on the NAC Profiler Server when integration is initially configured and communications between the systems established.

**Note** Prior to beginning this procedure, the password for the root system user account for the NAC Manager appliance (appliances for NAC Manager HA-pairs) must be determined. The script must be able to establish an SSH session with the NAC Manager as the root system user to successfully complete the setup which will require the user to provide the NAC Manager root password as the script executes.

**Step 1** Log on to the NAC Profiler Server via SSH (or from a console session) as the 'beacon' system user. For HA-pairs, initiate the session using the DNS name or IP of the VIP for the pair so the script is executed on the Primary node.

**Step 2** Execute the following variant of the service profiler commands:

```
[beacon@QAProfiler2 ~]$service profiler setupccakey
```

**Step 3** Follow the instructions provided on-screen to complete the configuration of SSH key-based authentication. During the run of the script the user will be prompted to enter the password for the root system user on the NAC Manager twice. The root password must be entered correctly for the setup to complete successfully.

If the setup is successful, the script will display NAC Manager information at the NAC Profiler command line read from the NAC Manager over the SSH tunnel. This verifies successful setup on the node. The following is an example of the output from this check as the script completes successfully:

```
NAC Appliance Software Information, read from CAM:

VERSION=4.5.0
NAME=Clean Access Manager
DATE=2008/10/20


*  Complete:  Key-based auth setup between Profiler
*               and CAM node cam4o.bspruce.com
```

**Note** When the NAC Manager is implemented as an HA-pair, the script will complete the setup on the Primary NAC Manager node first, and then repeat the steps to complete the setup of the Secondary node in the NAC Manager pair. Follow the on-screen messages carefully to ensure that setup completes on **both** members of the NAC Manager pair which enables the synchronization to function normally regardless of which NAC Manager appliance is the Primary node after setup. Similarly, if the NAC Profiler Server is a HA-pair as well, the script will detect the presence of the HA configuration and repeat the setup of keyless SSH on the Secondary node of the Profiler pair as well. In implementations where the NAC Manager and NAC Profiler Server are both deployed as HA-pairs, a total of **four** keyless SSH setups is required and performed iteratively by the scripts.

**Note** If a long delay is experienced during each attempt to log onto the NAC Manager, this indicates the NAC Profiler Server and/or the NAC Manager have not been configured with a name server (DNS resolver).Make sure to configure DNS name resolution for both the Cisco NAC Manager and Cisco NAC Profiler. (To configure name service on Cisco NAC Profiler use the `service profiler setupnetwork` command from the CLI, and for the NAC Manager utilize the web interface). If DNS is not available or desirable, you can alternatively add entries to the /etc/hosts files, creating a IP address-to-name mapping for each system's respective neighbor (i.e. add a NAC Manager entry to NAC Profiler Server's host file, and a NAC Profiler Server entry to the NAC Manager hosts file).

**Note** If the Address parameters for the NAC Manager in the NAC Profiler Server configuration are ever changed (from IP to DNS, or the reverse, or to just a different host address) then the SSH setup script needs to be rerun as described in this section. Similarly if the NAC Profiler Server is re-imaged, or an appliance is replaced, the script must be re-run to re-establish SSH between the Profiler Server and the NAC Manager service.

At the completion of the setup of SSH key-based authentication, return to the NAC Profiler UI and proceed to the Profiler Events page and select Create NAC Events to complete the next step of the integration configuration by creating required NAC Events as described in the next section.

# Creating NAC Events

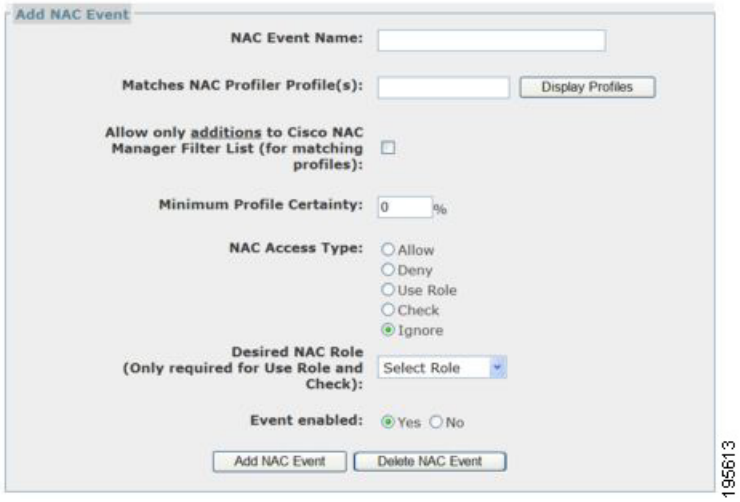
Through the creation of NAC Events, NAC Profiler is configured with information needed to populate and maintain the Filter List in the NAC Manager. The NAC Events specify which endpoint profiles contain endpoints that should be populated to the NAC Manager Device Filter list, and specify the required attributes for the entry: Access Type and Role (when applicable) that should be made in the Device Filter list entry made for each endpoint in the matching profile.

Typically, NAC Events are created to match the Cisco NAC Profiler profiles that contain endpoints that are known to be not NAC-compatible (see beginning of this chapter for discussion of "non-NAC" endpoints). The NAC Event essentially configures Cisco NAC Profiler to **populate** and **maintain** the Filter List in the NAC Manager by designating the Profile or Profiles that need to be accommodated via "white-listing" in the NAC Manager. This level of Cisco NAC Profiler integration with Cisco NAC Appliance fully leverages the Endpoint Profiling and Identity Monitoring functionality outlined in this guide.

Commonly, an individual Cisco NAC Event is added to the system configuration for each Profile containing devices to be populated in the NAC Manager, specifying the Profile by name. Alternatively, as detailed below, multiple Endpoint Profiles can be handled by a single Cisco NAC Event by matching these Profile names via use of a Regular Expression.

To create Cisco NAC Events, navigate to the Configuration tab, select the Events link from the secondary menu. Select the Create NAC Events link in the Profiler Events table. Figure 13-2 shows the form displayed on the page that opens in the browser upon selection of the Create Cisco NAC Events link:

***Figure 13-2 Add NAC Event Form***




Complete the following steps using the form to create a new Cisco NAC Event:

**Step 1** Specify the NAC Event Name for the new NAC Event

Enter a unique name for the NAC Event that will be meaningful to the administrators of the system.

**Note** The NAC Event Name is used to populate the Description field of the Device Filter List viewable in the NAC Manager for each endpoint added to the table via the integration with Cisco NAC Profiler. Use of a descriptive name indicates the NAC Profiler profile/type of device is recommended for ease of interpretation by the administrator and operators of the Cisco NAC Appliance system integrated with Cisco NAC Profiler.

**Step 2** Enter Endpoint Profile name (or RegEx) in Matches NAC Profiler Profile(s) field.

**Tip** Note the Display Profiles button on the form. Pressing this button results in the display of all currently enabled Endpoint Profiles, enabling "cut & paste" of Profile names into the Add NAC Event form.

This field is used to specify the endpoint Profile name (or a Regular Expression that matches names of one or more endpoint Profiles) containing the endpoints that will be sent to Cisco NAC Appliance for automatic population in the NAC Manager Device Filter List via this event. Typically, the matching profiles in a Cisco NAC event contain endpoints that will be provisioned with network access without being forced to authenticate and or be postured through Cisco NAC Appliance. In addition, Cisco NAC Profiler will monitor the identity attributes of the endpoints in the designated Profile(s); if an endpoint transitions to a new Profile, and there is not a NAC Event associated with the new Profile, it will be removed from the Device Filter list on the NAC Manager (Assuming the "Allow only additions…" option in the NAC Profiler Server configuration is not selected.)

**Note** The Matches NAC Profiler Profile(s) field will accept a Regular Expression to enable matching multiple Profile names with a single NAC Event. For example, to match all Profiles that have the string "IP Phone" in the description, use the following Regular Expression /ip phone/i.

**Note** You must add a forward slash ("/") at the beginning and end of the Profile name you enter in the Matches Profiler Profile(s): field of the Add NAC Event form to create a valid NAC Event. For example, **/Printers/** is a valid entry, while **IP Phone** is not.

**Note** For more information on Regular Expressions, see the following web references:
http://www.regular-expressions.info/

**Step 3** Select Allow only additions to NAC Manager Filter List Option as desired for this Cisco NAC Event

This option allows for setting of the "allow only additions" option at the Cisco NAC-event level. Like the similar Server (global) option discussed in the last section, selecting this option at the Cisco NAC event-level results in the Device Filter list entries populated by this NAC event to not be subjected to deletion from the Filter List or modification of the Access Type via NAC Profiler interaction. This allows the endpoints in selected profiles to be provided immunity from future synchronization actions other than update of the description field

**Note** "Allow only additions" at the NAC Event level is accomplished by the use the special Filter List description field prefix character of '*' that instructs the integration layer code to allow no updates to this entry except to its Description field. The description may change if the Profile of an endpoint changes, but the entry may not be deleted, nor its access type modified by NAC Profiler subsequent to its initial addition to the Filter List. This effectively disables the Identity Monitoring function for endpoints added to the Filter List via a NAC event with this option enabled, and in addition will not subject these endpoints to modifications to other than the Description field that might occur during a regular synchronization to include endpoints that are retired due to expiry of the Endpoint Timeout.

**Step 4** Set Minimum Profile Confidence option as desired.

Specify the minimum certainty value that is required for endpoints assigned to Profile(s) before the NAC Event action should be triggered (creating an entry in the NAC Manager filter list). For example, if this value is set at 40% then an endpoint matching a relevant Profile with certainty of only 35% would not trigger the defined action. The certainty value for an endpoint in a profile is a function of the rules in the Profile the endpoint has satisfied at that point in time as described in detail in Chapter 9, "Endpoint Profile Configuration: Part 1" on the configuration of Endpoint Profiles. This value is particularly pertinent for Profiles with multiple profile rules which by definition may have endpoints in them at different levels of certainty.

The default value for this parameter is 0, which is interpreted as any certainty

**Step 5** Set NAC Access Type.

Specify the Access Type of each NAC Device Filter List entry that should be created for endpoints added to the Device Filter List via this Cisco NAC Event. The choices are: Allow, Deny, Role, Check or Ignore.

For further details on Device Filters, refer to the "Device Management" chapter of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*.

**Step 6** Desired NAC Role.

This field is only required if NAC Access Type is set to either Role or Check. Select the appropriate NAC User Role to be specified in NAC Manager Filter List entries when the NAC Event is triggered. For all other Access Types (Allow, Deny, Ignore) this field is ignored.

**Note** The drop down list for Desired NAC Role in the Add NAC Event form is populated via the NAC Profiler Server configuration parameters. In order for NAC Profiler NAC Events to be configured to assign NAC Roles for endpoints with Access Types of Role or Check Access, these roles must be specified in the NAC Profiler Server Module configuration in the field entitled NAC Roles. See NAC Profiler Server Module Configuration, page 11-4 for instructions on configuring the NAC Profiler Server module parameters for NAC integration.

**Step 7** Event Enabled.

Once defined, the Cisco NAC Event can be enabled or disabled at any time by selecting the radio button of the desired option.

**Step 8** Add NAC Event.

Select the Add Cisco NAC Event button to save the NAC Event to the NAC Profiler system configuration.

Repeat the process above to add any additional Cisco NAC Events to the system configuration as required to designate the other endpoint profiles containing endpoints that should be populated on the NAC Manager Device Filter list.

**Note** The matching profiles for enabled NAC Events can be verified easily by viewing the Endpoint Directory (Endpoint Console -> Endpoint Directory). When an endpoint profile matches an enabled NAC Event, the NAC Event Name and minimum certainty will show in the NAC column of the Endpoint Directory in the row for the matching profile. See Figure 13-3 below.

*Figure 13-3 Endpoint Directory Showing Profiles Matching NAC Event*


# Synchronizing Cisco NAC Profiler and the NAC Manager Device Filter List

From time to time it is necessary to synchronize Cisco NAC Profiler with the NAC Manager to ensure consistency between systems. Performing a full synchronization ensures that the endpoints currently in Profile(s) that match an enabled NAC Event are consistent with the current Device Filter List populated in the NAC Manager and the Access Type(s) of the Filter List.

An example of when full synchronization is required is immediately after the enablement of the integration layer as outlined in this chapter in the preceding sections. This initial full synchronization will result in the endpoints currently profiled into profiles that match enabled NAC events to be provisioned to the NAC Manager Device Filter List with the attributes specified in the Cisco NAC events.

Also, anytime the Cisco NAC Events configuration is modified: Cisco NAC Events added, deleted or existing NAC Events modified, a full synchronization should be executed once the changes to the Cisco NAC Event configuration have been saved. Commanding a full synchronization causes NAC Profiler to evaluate all the endpoints it believes should be on the Filter List based on the most current NAC Event configuration with the current NAC Manager Filter List and make updates accordingly. The full synchronization process is initiated from the NAC Profiler user interface via the Apply Changes -> Update Modules or Apply Changes -> Re-Model. Whenever an Update Modules or Re-model is performed via the NAC Profiler user interface a full synchronization is performed by the integration layer.

The full synchronization process results in the NAC Profiler Server building-out a list of all endpoints currently in Profiles that match the enabled NAC Events in the system configuration. It then looks for a Filter List entry on the NAC Manager for each of the endpoints that are on that list and checks each for consistency with the parameters specified in the appropriate NAC Event (for example, Description, Access Type, Role if applicable, etc.) matching the Profile of that endpoint.

This ensures consistency between the Cisco NAC Profiler data and what is currently entered in the NAC Manager for all endpoints added to the Filter List via the integration. Entries in the Device Filter list can be designated to have parameters such as portions of the description and Access Type not subjected to the synchronization process in scenarios where some manual administration of the NAC Manager Device Filter List is used in conjunction with the Cisco NAC Profiler integration. See "Synchronization and Manually Created/Edited Filter List Entries" section on page 13-14.

In the second phase of the full synchronization process, the Cisco NAC Profiler will examine entries on the Filter List for endpoints **not** on the list compiled in the first step. These are endpoints that are on the Filter List and that according to the Cisco NAC Profiler's most current data, are not currently in a Profile that matches a NAC Event and therefore should not be on the Filter List.

If these endpoints do not have a special character in the leading character of the description field (see "Synchronization and Manually Created/Edited Filter List Entries" section on page 13-14) which designates that they should not be removed by the synchronization process, they will be deleted from the Filter List. Entries are marked in this manner either by the NAC Manager administrator, or result when entries are made by Cisco NAC Profiler resulting from endpoints being in profiles that have the NAC Event-level allow only additions option enabled.

Note that on NAC Profiler systems that have the global Allow Only additions option enabled (checked on in the Profiler Server configuration), this second phase of full synchronization is not performed in its entirety: no entries made by Cisco NAC Profiler will be removed from the NAC Manager Device Filter List. All endpoints added to the NAC Manager Device Filter list by the Cisco NAC Profiler with this option enabled globally are effectively immune from removal. However, the Description field of entries may be modified so that it is consistent with the NAC Profiler data at the time of the synchronization.

**Note** When the Allow Only Additions option is enabled in the NAC Profiler Server configuration so that all entries added to the NAC Manager are handled in this manner, omitting the second phase of synchronization is done programatically and not via pre-fixing the entry with the special character. Unlike entries resulting from NAC Events with the event-level Allow Only Additions option checked, there will be no "*" in the first character of the description field for NAC Manager Device Filter list entries made by a NAC Profiler system with the Allow Only Additions option checked in the Server configuration.

# Synchronization and Manually Created/Edited Filter List Entries

In implementations where the Cisco NAC Profiler is providing all management of the NAC Manager Filter List, and manual intervention by network operation personnel does not occur, the normal interaction of the systems via the automated synchronization process described earlier in the chapter is sufficient for ensuring the Filter List is kept current.

Through the integration processes, Cisco NAC Profiler is able to add entries to the NAC Manager Device Filter list, as well as modify or delete any Filter List entry it has made previously when the endpoint is re-profiled or retired. Cisco NAC Profiler provides all required administration of the NAC Manager Device Filter List.

In some cases it is desirable for the administration of some NAC Manager Device Filter list entries to be performed manually, and to have some or all of the entries made manually immune to the synchronization process. During Cisco NAC Profiler/Cisco NAC Appliance synchronization, by default all entries in the Filter List are subject to modification and or removal--whether they are made by Cisco NAC Profiler or made manually via the NAC Appliance user interface.

Unless the Allow only additions option is enabled globally resulting in all entries being immune to removal, or selected entries made immune through the event-level allow only setting, the Cisco NAC Profiler synchronization process will consider every entry on the NAC Manager Device Filter List subject to modification/removal. This default behavior however may be modified on a per-entry basis by signifying that designated NAC Manager Device Filter list entries should be handled differently by the automatic synchronization process in cases where the entry has been determined by higher authority to be correct as currently entered.

This is accomplished via the optional use of reserved prefix characters in the initial character positions of the Filter List description field of the Filter List entry. Table 13-1 lists the reserved prefix characters, and the modification to synchronization that will occur if these characters are encountered by the synchronization process as the initial characters of the description field of a Filter List entry are processed:

***Table 13-1 Reserved Characters***

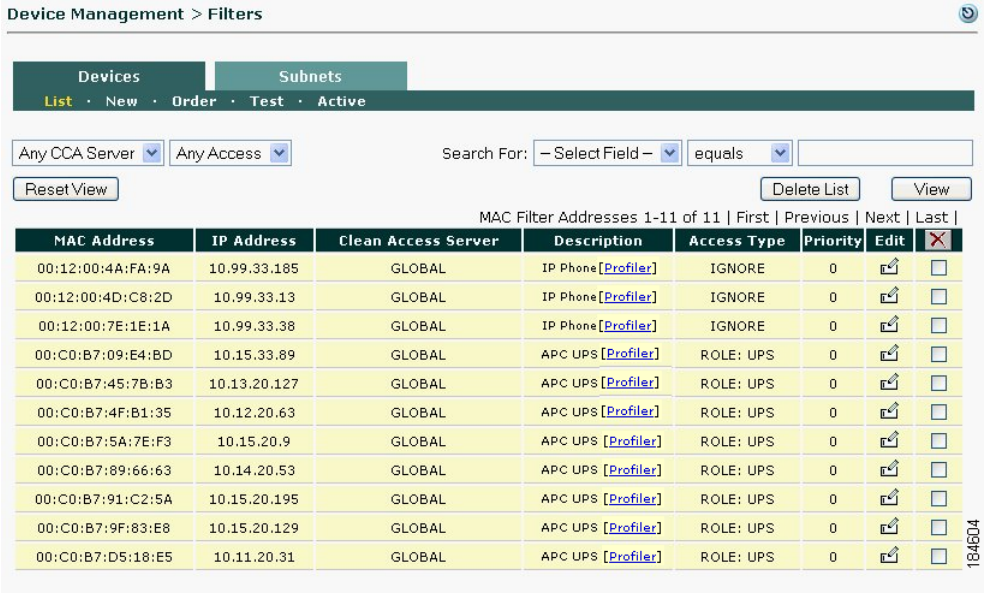
| Reserved Character | Name | Effect on Synchronization Process |
|---|---|---|
| + | Custom Comment | Indicates that custom comment text follows that is to be maintained permanently. During the synchronization process, Cisco NAC Profiler may update the description field (and all other fields) but the description text entered after the + symbol will be preserved. |
| * | Locked Access | Has the same effect as the + prefix in regards to the description field and in addition, this prefix will instruct the synchronization process that:<br>• The entry may not be deleted.<br>• The Access Type of the entry may not be modified.<br>The synchronization process can only update the description field of Locked Access entries |
| ** | Frozen | Indicates that this entry may not be deleted or modified in any way by the synchronization process. In effect, it is a permanent entry unless modified manually. Frozen entries are totally immune to the synchronization process. |

# Verifying Cisco NAC Profiler/Cisco NAC Appliance Integration

To verify that Cisco NAC Profiler is populating entries properly in the Device Filter list of the NAC Manager, log into the NAC Manager as administrator. Select the Filters button under Device Management in the left-hand navigation bar. The following screen displays in the main pane of the browser, enumerating all the endpoints currently on the NAC Manager Device Filter list.

After configuring the NAC Profiler Server NAC Appliance integration parameters, establishing SSH with the NAC Manager, adding NAC Events, and performing a full synchronization process, the endpoints that are in the Profile(s) matching enabled NAC events should be populated to the device filter list of the NAC Manager.

*Figure 13-4 NAC Manager Device Filter List*



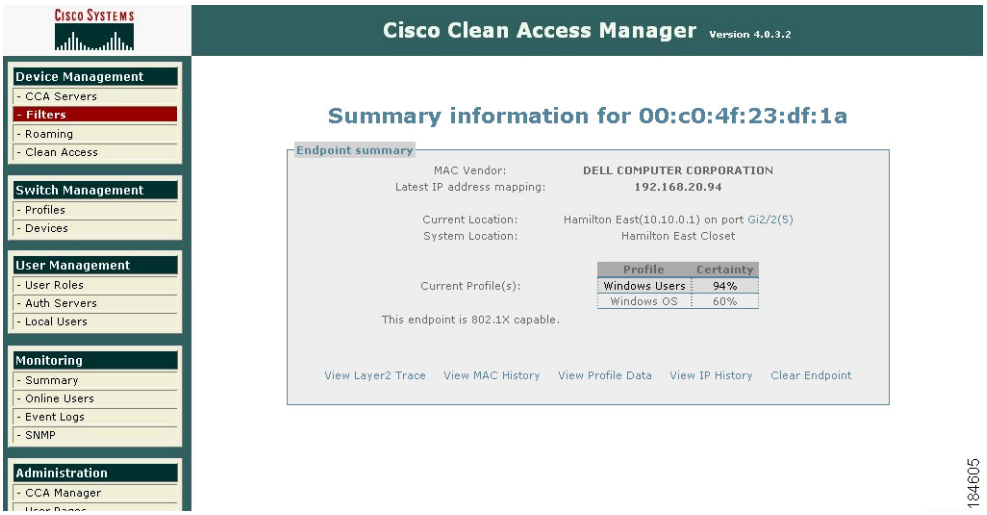

Endpoints that have been added to the Device Filter list on the NAC Manager via the integration with Cisco NAC Profiler are prominently marked by the **Profiler** link in brackets following the respective NAC Profiler event name that resulted in the endpoint being added to the Device Filter list. Recall that one or more endpoint profiles are defined as matching when creating a NAC Event.

The NAC Event Name therefore implies that the endpoint is currently in a Profile that matches the NAC Event specified in the description field of the Device Filter list entry. The MAC Address, IP Address, NAC Server, Description and Access Type fields are populated by Cisco NAC Profiler for each endpoint added to the Filter list via the integration layer.

The link following the text in the description field is a hot-link to a summary of all available information (real-time and historical) about the endpoint being maintained by Cisco NAC Profiler. Selecting the NAC Profiler link from the NAC Manager displays this summary page, from the administrator's perspective, within the context of the NAC Manager web interface.

This allows easy access to endpoint location information (if known), current profile, MAC and IP history, and a Layer 2 trace details – all displayed directly from within the NAC Manager GUI, providing access to all contextual data gathered by Cisco NAC Profiler from a single unified interface. (Full information regarding endpoint summary views is provided in Chapter 15, "Using the Cisco NAC Profiler Endpoint Console").

*Figure 13-5 Viewing Cisco NAC Profiler Endpoint Data from a NAC Manager*




# Cisco NAC Integration Log Messages

With the verbose logging option enabled in the NAC Profiler Server configuration, activity of the NAC Appliance integration layer is maintained in the Server log which is viewable from the NAC Profiler user interface. Navigate to the Utilities tab, select System Summary link from secondary menu, then select the View Server Log button.

The log entries associated with the NAC integration layer are prefixed with NAC_SYNC.

Entries associated with a full synchronization, which occur each time the system is restarted via Apply Changes -> Update Modules, or Re-model and automatically every sixty minutes will appear in the logs as follows:

```
NAC_SYNC: Profiler / NAC Synchronization END [add 0, upd 0, desc 0, rm 0]
NAC_SYNC: Profiler / NAC Synchronization START
```

The END message includes a summary of changes made during the synchronization: entries added (add), entries updated (upd), description changes (desc) and entries removed (rm).

While in dynamic event handling mode, as endpoints enter or leave profiles matching enabled NAC Events, entries such as the following are made to the Server log:

```
NAC_SYNC: [addmac 00:b0:19:00:00:01] Success
NAC_SYNCH: [removemac 00:b0:19:01:aa:02] Success
```

# View/Edit NAC Events List

To view the list of existing NAC Events on a Cisco NAC Profiler system, select the Configuration Tab from any page of the Cisco NAC Profiler web interface. Select the Events link from the Configuration tab secondary menu, and then select View/Edit NAC Events. A new page containing the Table of NAC Events displays in the browser, as shown in Figure 13-6.

*Figure 13-6 Table of NAC Events*

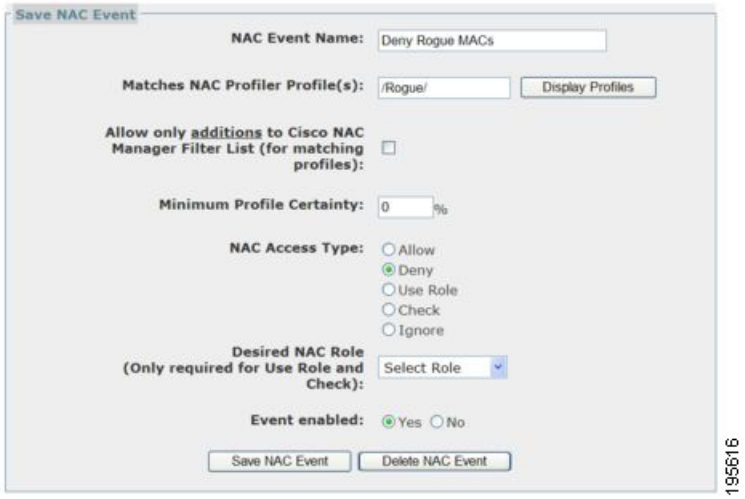

The table provides a summary view of NAC Events currently saved to Cisco NAC Profiler configuration. The table displays the name, the Profiles applicable to the NAC Event, the Access Type specified for Device Filter List entries made by the Cisco NAC Profiler NAC Event in the NAC Manager, and current status of the Event (enabled/disabled) for each NAC Event.

For NAC Events with the Access Types of Role and Check, the configured NAC role is shown in parenthesis after the words Role or Check. The Regular Expression specified in the NAC Event "Matches NAC Profiler Profile(s) field is displayed in the Profile column of the Table of NAC Events.

If a Minimum Profile Certainty is specified for the NAC event, it is shown immediately after the Matching Profile regex in parenthesis. For example in Figure 13-6, the Regular expression /phone/i results in endpoints being Profiled into any NAC Profiler Profile with a Profile Name containing the string 'phone' (regardless of case) with confidence equal to 20% or greater being added to the Device Filter List of the NAC Manager.

The displayed NAC Event names are links. Selecting a NAC Event Name results in the Save NAC Event form being displayed as shown in Figure 13-7.

*Figure 13-7 Save NAC Event Form*




Through the Save NAC Event form for a saved NAC Event, changes to any of the parameters of the NAC Event can be made and subsequently saved to the system configuration.

See Creating NAC Events, page 13-10 for detailed descriptions of each of the NAC Event configuration parameters.

After making any changes to the configuration parameters of a NAC Event, select the Save NAC Event button at the bottom of the form to commit the changes to the configuration. Existing NAC Events can be deleted from the configuration if desired by selecting the Delete NAC Event Button at the bottom of the Save NAC Event form.

# Troubleshooting Cisco NAC Appliance Integration

For Cisco NAC Profiler/Cisco NAC Appliance integration to function properly it must be configured correctly, as described previously, and several outside dependencies must be satisfied, including:

- No barriers (for example, firewalls or ACLs) to network communication between the NAC Profiler Server and the Cisco NAC Appliance NAC Manager.
- Correct configuration of Cisco NAC Appliance NAC Manager administrator web credentials in the Profiler Server module (or other admin account with “full-control” API access).
- Correct configuration of SSH key-based authentication between the beacon system user on NAC Profiler and the “root” system user account on the NAC Manager.

The following is a list of measures that can assist in efforts to troubleshoot situations where the integration is not working as expected.

## Verify Network Communications

Log into the Profiler Server (console or SSH) and use the following techniques to verify that required network communications between the systems is currently functional. If the NAC Profiler Server is implemented as an HA pair, begin this procedure from the current primary for the system. If connecting via SSH, establish the SSH session with the VIP.

1. Establish that the Profiler Server appliance can communicate with the NAC Manager over the network:

   ```
   $ ping <NAC Manager-IP>
   $ traceroute –n <NAC Manager-IP>
   ```

2. Verify API communication

   ```
   $ telnet <NAC Manager-IP> 443
   ```

   Successful establishment of a telnet session is typically indicated by the following messages:

   ```
   Trying <NAC Manager-IP>...
   Connected to <NAC Manager-IP>.
   Escape character is '^]'.
   (to exit, hit CTRL-], type “quit” and hit ENTER)
   ```

3. Verify SSH key-based authentication setup

   ```
   $ ssh root@<NAC Manager-IP> ls /
   ```

   If SSH key-based authentication is functioning correctly then a directory from the NAC Manager root directory will be shown, with no prompting for password.

**Note** If the NAC Profiler system is unable to establish the SSH connection with the NAC Manager for the synchronization, a message similar to this one will appear in the Server log each time the system is restarted, or when the automatic hourly synch is attempted:

```
NAC_SYNC: CAM ssh connect failure to host cam4o.bspruce.com
```

If the systems are unable to communicate with one another over the network using ping or telnet, it is likely that there are measures in place such as a firewall or router ACL preventing that communication. Consult with the network operations or security group to determine what is preventing the devices from establishing communications over the network. If practical, have those measures adjusted to enable communications between Cisco NAC Profiler and the NAC Manager, or consider moving the systems onto the same network segment.

If the attempt to ssh to the NAC Manager as the root system user requires the entry of the NAC Manager root password at the command line, this indicates failure of the keyless SSH setup that should have been run during setup of integration with the NAC Appliance system. See Configure Key-based SSH Authentication, page 11-7.

**Note** If either the NAC Profiler Server and or the NAC Appliance NAC Manager is an HA-pair, it is important to establish that this connectivity is possible for all systems. When the NAC Profiler Server is implemented as a HA-pair, perform these checks on both the Primary and Secondary modes. If the NAC Manager is an HA-pair, verify connectivity to both nodes in the NAC Manager pair.

# Integration Debug Logs

The system log may be examined for entries related to integration with Cisco NAC Appliance via the command line. As described earlier the log entries related to the NAC integration layer actions will be prefixed with NAC_SYNC.

The following are typical commands that may be used for viewing these log entries from the command line of the NAC Profiler Server integrated with NAC Appliance:

1. Show all related log messages to date

```
$ grep NAC_ /usr/beacon/logging/Server.out | less
```

2. Watch related log messages as they happen

```
$ tail -f /usr/beacon/logging/Server.out | grep NAC_
```

# Use of “Custom API” Feature

The Custom API option of the Server module NAC configuration (Configuration -> Profiler Modules -> Server -> NAC Configuration) should only be implemented in specific situations as described in this documentation, or as directed by the Cisco TAC. Whenever upgrading Cisco NAC Profiler or Cisco NAC Appliance software, carefully consult the release notes to determine if it is appropriate for the Custom API to be enabled.

The Custom API functionality was implemented to provide extensions to the Cisco NAC Appliance API for three specific scenarios:

- Scenario A: Cisco NAC Appliance 4.0, Access Types CHECK and IGNORE, page 13-21
- Scenario B: Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2, Out Of Band deployments, page 13-21
- Scenario C: Cisco NAC Appliance 4.1.3, Out Of Band deployments, page 13-21

## Scenario A: Cisco NAC Appliance 4.0, Access Types CHECK and IGNORE

The API for Cisco NAC Appliance release 4.0 does not support Device Filter List access types CHECK and IGNORE. If either of these access types is to be used with NAC-Event-Rules, then the Custom API must be enabled, using patch file **cca4_api_addmac.diff**.

## Scenario B: Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2, Out Of Band deployments

For Out Of Band (OOB) deployments, switch port VLAN provisioning typically immediately enforces updates to the Device Filter List as soon as they are made. In other words, the assigned VLAN on a port should immediately be updated if a Device Filter List entry, which specifies the MAC address for an endpoint connected to the given port, is added, removed, or changed. For OOB deployments with Cisco NAC Appliance releases 4.1.0, 4.1.1, 4.1.2, the immediate enforcement of network access policy via Device Filter List changes does not occur. For example, if a printer is already connected to the network and a Device Filter List entry for the printer's MAC address is added, the printer is not immediately granted network access (nor is access immediately revoked if the Filter List entry is removed).

If this behavior is desired when running Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2, the Custom API must be enabled, using patch file **cca41x_api_bounceport.diff**.

**Note** This mode of Custom API use has been tested and approved for use with the following Cisco NAC Appliance releases:

- Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2
- If using release 4.1.0 or 4.1.1, patching of ssl.conf is required as described in Implementation Instructions, page 13-21, and Important Caveat, page 13-23.

## Scenario C: Cisco NAC Appliance 4.1.3, Out Of Band deployments

This scenario is similar to Scenario B: Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2, Out Of Band deployments, page 13-21, but affect Cisco NAC Appliance 4.1(3).

For this scenario no patch file is utilized. For implementation, simply enable the Custom API check box in the Profiler Server Configuration as described in Step #2 in the implementation instructions below.

**Note** This mode of Custom API use has been tested and approved for use with the following Cisco NAC Appliance release:

- Cisco NAC Appliance 4.1.3

## Implementation Instructions

For the following instructions:

- PATCH_FILE is the selected patch file named in the corresponding section
- NAC Manager is the IP or DNS address of the NAC Manager system (VIP/service address for HA NAC Manager pairs).

Perform the following steps to enable the Custom API.

## Prerequisite

Configure Cisco NAC Profiler integration with Cisco NAC Appliance as described in Configuring Cisco NAC Appliance Integration, page 13-4 before enabling the Custom API.

## 1. For Scenarios A and B ONLY: Patch API file

Log on to the Profiler Server via SSH as the beacon system user and perform the following commands.

**Note** Be especially careful with the last command.

```
1. profiler# cd /usr/beacon/etc
2. profiler# scp root@NAC
Manager:/perfigo/control/tomcat/normal-webapps/admin/cisco_api.jsp cisco_api.jsp
3. profiler# patch -b < cca_api/PATCH_FILE
4. profiler# scp cisco_api.jsp root@NAC
Manager:/perfigo/control/tomcat/normal-webapps/admin/cisco_api_alt.jsp
```

## 2. For ALL Scenarios: Tun on Feature in Profiler Server UI

In the Cisco NAC Profiler Server web interface, do the following:

**Step 1** Browse to Server module configuration screen by navigating to Configuration-> NAC Profiler Modules->List NAC Profiler Modules->"Server"

**Step 2** In the "NAC Configuration" section, enable the check box labeled Custom API

**Step 3** Click Update Server

**Step 4** Restart the Server module: Configuration->Apply Changes->Re-Model

## 3. Scenarios B and C on Cisco NAC Appliance 4.1.0, 4.1.1: Patch ssl.conf

**Note** This step is required for Scenario B: Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2, Out Of Band deployments, page 13-21 andScenario C: Cisco NAC Appliance 4.1.3, Out Of Band deployments, page 13-21 when the Cisco NAC Appliance release is 4.1.0 or 4.1.1 only. This step is not required for release 4.0 or 4.1.2 and later.

Log on to the Profiler Server system via SSH as beacon system user and perform the following commands:

```
1.      profiler# cd /usr/beacon/etc
2.      profiler# scp root@NAC Manager:/perfigo/control/apache/conf/ssl.conf ssl.conf
3.      profiler# patch -b < cca_api/cca41x_ssl_conf.diff
```

```
4.      profiler# scp ssl.conf root@NAC Manager:/perfigo/control/apache/conf/ssl.conf
5.      profiler# scp ssl.conf root@NAC Manager:/perfigo/control/apache/conf/ssl_alt.conf
6.      On NAC Manager, execute these commands:
7.      NAC Manager# /perfigo/control/bin/stopapache
8.      NAC Manager# /perfigo/control/bin/startapache
```

## Important Caveat

This setup will stop being operational if either the NAC Manager is rebooted or command 'server perfigo restart' is executed on the NAC Manager. If this happens, the following commands must be executed to restore the custom API to operational status.

```
NAC Manager# cd /perfigo/control/apache/conf/ssl_alt.conf
NAC Manager# cp ssl.conf.patched ssl.conf ssl.conf
NAC Manager# /perfigo/control/bin/stopapache
NAC Manager# /perfigo/control/bin/startapache
```

**Note** Upgrading to Cisco NAC Appliance release 4.1(2) or later removes the need for this NAC Manager ssl.conf file workaround.