# Integration with 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 Behavior Monitoring with Cisco NAC Appliance provides several distinct advantages in the deployment and ongoing operation of NAC Appliance in enterprise networks. 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 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 devices. The devices that cannot interact with NAC Appliance in the same way user devices such as desktop and laptop computers can, must be identified and added to a table in the Clean Access Manager (CAM). This table, accessible from the Device Management section of the CAM is commonly referred to as the Filter List. The Filter List is populated with the list of endpoints (by MAC address) that are known to require special handling by the NAC system in order to be admitted onto the network.

Endpoints that have their MAC addresses added to the Device Filter list in the CAM are handled by exception by the NAC system whenever these devices join the network. A device 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.

In the absence of the NAC Profiler, the initial population and ongoing management of endpoint entries in the Device Filter List is done manually in NAC Appliance deployments. This process requires not only the identification of the endpoints by MAC address, it requires each of the 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 getting stale as devices are retired or otherwise removed from the environment unless the list can be attended to on almost a daily basis. Understanding that the endpoints on the Device Filter list are essentially given an open door to the network for as long as their MAC address is on the list, and the fact that there is no mechanism built-into the NAC Appliance solution to police the activities of these devices, creates a potential weakness in the NAC Appliance solution that can only be addressed through regular and potentially intensive manual intervention that can be error prone.

The integration of Cisco NAC Profiler with NAC Appliance significantly enhances the ability to provide reliable and secure access to the NAC-enabled network while significantly decreasing administrative burden. NAC Profiler enables the automated detection and location of non-NAC endpoints across the entire network environment in which NAC Appliance will be deployed in an automated, highly accurate and non-intrusive fashion. NAC Profiler Profiles 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 CAM automatically, via the 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. As importantly, NAC Profiler has the ability to *remove* devices from the device filter list. This is the functionality provided by the Behavior Monitoring function of Cisco NAC Profiler. NAC Profiler is constantly monitoring the observable attributes of endpoint behavior such as the application-specific network traffic being generated by the endpoint, or markers of specific operating systems. When observations indicate behavior 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 containerize NAC-capable endpoints, NAC Profiler will remove the associated MAC address from the Device Filter list of the CAM. As the entry is removed from Filter List whatever network access privileges that had been assigned are revoked; for that endpoint to regain network access, it must undergo the full NAC authentication and posturing prescribed for NAC-capable endpoints. Essentially this functionality adds to the 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 behavior. NAC Profiler constantly monitors the behavior of each endpoint on the device filter list, ensuring that current behavior is consistent with previously observed behavior that had led to the endpoint being allowed onto the network without full NAC authentication and posturing.

NAC Profiler also monitors each endpoint in the database for activity on the network. Endpoints that have been removed from the network, indicated by a long lapse in network traffic sourced from the endpoint's MAC address and observed by NAC Profiler can also result in a change in Profile and the removal from the Device Filter list. In this manner, NAC Profiler is able to continually prune the Device Filter List of the entries for devices that are no longer in use automating this aspect of administration of the NAC Appliance system over its entire lifecycle.

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

# Configuration of NAC Appliance Integration

Configuration of the integration of the NAC Profiler Endpoint Profiler and Cisco NAC Appliance consists of two distinct steps.

**Step 1**    Provide the NAC Profiler Server with the information required for it to communicate with the CAM via the NAC Appliance API.

**Step 2**    Configure a special NAC Profiler event type, called a "NAC Event." NAC Events are essentially special-purpose Profile Change Events as described in Chapter 10, "Configuring 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 CAM.

# NAC Profiler Server Configuration

The primary task in this workflow consists of providing the Server module of Cisco NAC Profiler with the necessary information about the CAM in the NAC Appliance system to enable communications between Cisco NAC Profiler and the CAM via the API. Prior to beginning this step, collect the necessary information about the NAC Appliance configuration such as:

- IP address of the CAM.
- CAM web administrator username and password.
- NAC version.
- Any NAC Roles that might be assigned to non-NAC endpoints, applicable only for adding Device Filter entries with the Role or Check Access Type.
- The DNS domain-name of the NAC Profiler (alternatively, the IP address of Cisco NAC Profiler may be substituted, but this is not recommended).

## Configure SSH Key-Based Authentication

Before beginning the configuration of the parameters governing the integration of NAC Profiler and NAC appliance, complete this step to set up secure communications between NAC Profiler and the NAC Appliance CAM.

Log on to the NAC Profiler Server via SSH as username 'beacon' and execute the following commands:

```
profiler# cd /usr/beacon/etc
profiler# sh setup-CAM-key-auth.sh
```
Follow the instructions provided on-screen to complete the configuration of SSH key-based authentication.

**Note**    If a long delay is experienced during each attempt to log onto the CAM, this indicates that the NAC Profiler and/or the CAM have not been configured with a name server (DNS resolver). Configuration of name resolution for both the CAM and NAC Profiler are highly recommended. (To configure name service on the NAC Profiler, edit etc/resolv.conf, and for the CAM configure the web interface).

If DNS is not available, you can alternatively add entries to /etc/hosts files, creating an IP address-to-name mapping for each system's respective neighbor (for example, add a CAM entry to the Profiler's hosts file and a Profiler entry to the CAM hosts file).

# NAC Profiler Server Module Configuration

To configure the required NAC Profiler Server parameters for integration with a NAC appliance, go to the Configuration Tab, select NAC Profiler Modules, select List NAC Profiler modules, and then select the Server module name to bring up the Configure Server form. Scroll down the form to the parameter entitled "External reference," to enter the DNS domain-name or IP address of Cisco NAC Profiler. Figure 11-1 shows the NAC-specific parameters of the Configure Server form prior to the entry of any parameters for the environment.

*Figure 11-1    Server Parameters for Profiler Integration with NAC Appliance*



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

### External Reference

Enter the DNS domain-name (preferred) or IP address of the management interface 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 CAM Device Filter List. These web links give the administrator the ability to easily refer to NAC Profiler to find out more details about endpoints entered into the Device Filter List directly from the CAM interface.

### Username

Enter a valid Administrator user name that has been configured on the Clean Access Manager (CAM) server. NAC Profiler will use this name to gain administrator-level access to the CAM via the NAC Appliance API.

**Note**      An Administrator user can be created on the CAM that is specific to the NAC Profiler integration and that has only API-level administrative access. Refer to the Cisco NAC Appliance documentation for instructions on how to create a CAM administrator user with only API-level access. Note that the administrative user must be granted "full control" API access.

**Password**

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

**Address**

Enter the DNS domain-name of the CAM. Alternatively, if DNS is not set up for Cisco NAC Profiler or if a DNS address record has not been created for the CAM, the IP address of the CAM can be entered.

**Version**

Select the NAC version deployed from the drop-down menu.

**Allow only additions to CAM Filter List**

If selected, NAC Profiler will manage the Filter List on the CAM in the following manner: Once an entry has been created on the Filter List by NAC Profiler, the Profiler will **not** delete the entry nor modify the access type of the endpoint. Effectively, selecting this option disables the Behavior Monitoring function of NAC Profiler.

Note that although this option is selected, NAC Profiler can still make changes to the description field in the Filter List, in particular changing the Profile recorded in the description of an endpoint should its behavior 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 behavior.

**Perform Synchronization during 'Update Modules'**

This option controls the behavior of the Synchronization function between the NAC Profiler and NAC appliance. If selected, any time an Apply Changes -> Update Modules or, Apply Changes -> Re-model is executed at the NAC Profiler Server, a full synchronization between NAC Profiler and the CAM will be executed as described in Synchronizing NAC Profiler and the CAM Filter List, page 11-9.

Regardless of the setting of this parameter, per NAC-Event-Rule synchronization is always available as described in Creating NAC Events, page 11-6.

**Custom API**

This checkbox is used to enable the use of an alternate customized NAC Appliance API. This advanced feature should only be enabled if specified in release notes that accompany an upgrade to the NAC Profiler, or as directed by Cisco Systems technical support.

**Verbose Logging**

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

**NAC Roles**

This field is only required if network access to be provisioned to non-NAC endpoints will be differentiated via the NAC Appliance "User Role" construct. Each entry in the CAM filter table has an "Access Type" attribute that specifies the type of network access to be applied for the given endpoint. If 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 defined on the NAC Appliance system that could be assigned to non-NAC endpoints. If NAC Profiler will only add entries with the "Ignore", "Allow" and "Deny" Access Types this field should be left blank. (See the Cisco NAC Appliance documentation for a discussion of Access Types and User Roles – also see following discussion of NAC Profiler NAC Event.)

At the completion of these steps, the Server module configuration for NAC Profiler 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 to the Profiler Events page and select Create NAC Events to complete the second step of the configuration workflow described in Creating NAC Events, page 11-6.

# Creating NAC Events

Through the creation of NAC Events, Cisco NAC Profiler is configured with information needed to populate and maintain the Filter List in the CAM. Each NAC Event that is defined specifies a type endpoint access to be provisioned for a certain subset of endpoints: endpoints that NAC Profiler has categorized into one or more Profiles of interest. Typically, these would be Profiles that contain devices that are known to be not NAC-compatible (see beginning of this chapter for discussion of "non-NAC" endpoints). The NAC Event essentially configures NAC Profiler to **populate** and **maintain** the Filter List in the CAM by designating the Profile or Profiles that need to be accommodated via "white-listing" in the CAM. This level of NAC Profiler integration with NAC Appliance fully leverages the Endpoint Profiling and Behavior Monitoring functionality outlined in the first chapter.

Commonly, an individual NAC Event is added to the system configuration for each Profile containing devices to be populated in the CAM, specifying the Profile by name. Alternatively, as detailed below, multiple Profiles can be handled by the same NAC Event by matching these Profile names via use of a Regular Expression (similar to a wildcard expression, but much more flexible).

To create NAC Events, select the Create NAC Events link in the Profiler Events table. The following form is displayed on the page that displays in the browser upon selection of the Create NAC Events link:

*Figure 11-2        Add NAC Event Form*



Complete the following entries in the form to create a new NAC Event:

### NAC Event Name

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 CAM for each endpoint added to the table via the integration with 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 NAC Profiler.

### Matches Profiler Profile(s)

This is the Profile name (or a Regular Expression that matches names of closely related Profiles) containing the endpoints that will be sent to NAC Appliance for automatic population in the CAM Device Filter List. Typically, these will be the Profile or Profiles containing devices that will be provisioned with network access without being forced to authenticate and or be postured through NAC Appliance. In addition, NAC Profiler will monitor the behavior 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 CAM (Assuming the "Allow only additions…" option in the Server module 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, **/NoAuth/** is a valid entry, while **NoAuth** is not.

**Note**    For more information on Regular Expressions, see the following web references:
http://www.regular-expressions.info/
http://www.cs.tut.fi/~jkorpela/perl/regexp.html
http://www.ilovejackdaniels.com/cheat-sheets/regular-expressions-cheat-sheet/

### Allow only additions to CAM Filter List

This option allows for setting of the "allow only additions" option at the NAC-event level. Like the similar Server option discussed in the last section, selecting this option for a NAC event 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.

**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 Behavior 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.

**Minimum Profile Confidence**

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 CAM 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 is derived from the rules bound to each Profile as described in detail in Chapter 9, "Configuring Endpoint Profiles" on the configuration of Endpoint Profiles. This value is particularly pertinent for Profiles with multiple rules.

**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 rule. The choices are: Allow, Deny, Role, Check or Ignore.

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

**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 CAM 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 configuration in the field entitled NAC Roles. See NAC Profiler Server Module Configuration, page 11-4 for instructions on configuring the NAC Profiler Server parameters for NAC integration.

**Event Enabled**

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

**Add NAC Event**

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

Repeat the process above to add any additional NAC Events to the system configuration as required.

**Note**    Configuration changes made to NAC Profiler NAC Events are made active by selecting the Update Modules or Re-Model button on the Apply Changes page of the NAC Profiler web interface. To navigate to the Apply Changes page, select the Configuration tab from any page, then select Apply Changes from the left hand navigation options.

**Note**    If the Server option to perform synchronization during 'Update Modules' is enabled, a full synchronization as described in the next section will be performed.

# Synchronizing NAC Profiler and the CAM Filter List

Completion of the steps outlined above for Server module configuration and the addition of NAC Events as required has enabled NAC Profiler to begin managing the Device Filter List within the CAM. The integration is event-driven in that once the integration with NAC Appliance has been enabled correctly, as endpoints transition into Profiles named in NAC Events, those endpoints will be added to the Device Filter list on the CAM as they are added to the Profile.

From time to time it is necessary to synchronize NAC Profiler with the CAM to ensure there is consistency between systems. Essentially synchronization ensures that the endpoints that NAC Profiler currently has in Profile(s) that match an enabled NAC Event is consistent with what is currently populated in the Filter List especially with regard to Filter List settings such as Access Type. An example of when synchronization is required is the modification to an existing CCA Event such that an additional, already-enabled Profile with endpoints currently in the Profile is considered among the matching Profile(s) of the CCA Event. As described above, endpoints already in the Profile will not be added to the Filter List because of the event-driven nature of the integration. Performing synchronization causes NAC Profiler to evaluate all the endpoints it believes should be on the Filter List with the current Filter List and make updates accordingly.

The synchronization process is initiated in one of two ways. As described in the section outlining Server configuration earlier in this chapter, there is an option in the NAC Configuration to perform synchronization during Update Modules. Selecting this option results in a full synchronization process being performed any time either an Apply Changes -> Update Modules or Apply Changes -> Re-Model is performed on Cisco NAC Profiler. This is referred to as a full synchronization and is described as follows.

The full synchronization process results in the NAC Profiler building-out a list of all endpoints currently in Profiles that match the active NAC Events in the system configuration. It then looks for a Filter List entry on the CAM for each of the endpoints that are on that list and checks each for consistency with the parameters specified in the appropriate NAC Event (e.g., Access Type, etc.) matching the Profile of that endpoint. This ensures consistency between the NAC Profiler data and what is currently entered in the CAM 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 synchronization. See "Synchronization and Manually Created/Edited Filter List Entries" section on page 11-10.

In the second phase of the full synchronization process, the 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 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 11-10) which designates that they should not be removed by the synchronization process, they will be deleted from the Filter List.

Also, a manual, partial synchronization can be performed at the NAC Event level. After a NAC Event is saved and enabled in the system configuration, the Save NAC Event form is populated with an additional button entitled "Synchronize." To navigate to this form, go the Configuration Tab, select the Endpoint Events option, and then select View/Edit NAC Events. Selecting one of the configured and enabled NAC Events will display the Save NAC Event form for that event as shown in Figure 11-7.

*Figure 11-3        Save NAC Event - Synchronize*



Selecting the Synchronize button from the Save NAC Event form results in the synchronization occurring only for this NAC Event. This synchronization process is somewhat different than the full synchronization described immediately above. In NAC Event-level synchronization, the synchronization process considers only the Profiles that match the selected NAC Event. NAC Profiler will determine all endpoints that are currently in the Profile(s) that match that event only, check the Filter Table for each endpoint and ensure the entry for each endpoint in the matching Profile(s) is consistent with that specified in the NAC Event selected for synchronization. Also, phase 2 of the full synchronization process (during which entries may be removed from the Filter List) is not performed during a NAC Event-level synchronization.

# Synchronization and Manually Created/Edited Filter List Entries

In implementations where NAC Profiler is providing all management of the Filter List, and manual intervention by network operation personnel does not occur, the normal interaction of the systems via the synchronization process described above is sufficient for ensuring the Filter List is kept current. The full synchronization process has the authority to modify or delete any Filter List entry in addition to adding endpoints to the Filter List as described earlier in this chapter.

In some cases it is desirable for particular endpoints to be added to the Filter List manually, or modifications made to entries originally added by NAC Profiler. During NAC Profiler/NAC Appliance synchronization, by default all entries in the Filter List are subject to modification and or removal. This default behavior however may be modified on a per-entry basis by signifying that a given Filter List entry 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 11-1 lists the reserved prefix characters, and the modification to synchronization that will occur if these characters are entered as the initial characters of the description field of a Filter List entry:

***Table 11-1        Reserved Characters***

| Reserved Character | Name | Effect on Synchronization Process |
|---|---|---|
| + | Custom Comment | Indicates that custom comment text follows. During the synchronization process, 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. |
| ** | 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. |

# Verifying NAC Profiler/NAC Appliance Integration

To verify that NAC Profiler is populating entries properly in the Device Filter list of the CAM, log into the CAM 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 CAM Device Filter list.

After configuring the Server module parameters, adding NAC Events, and performing a Synchronization process (full or NAC Event level), the endpoints that are in the Profile(s) matching enabled (and synchronized) NAC events should be populated to the device filter list of the CAM.

***Figure 11-4        CAM Device Filter List***

Endpoints that have been added to the Device Filter list on the CAM via the integration with NAC Profiler are prominently marked by the **Profiler** link in brackets following the respective Profile name. The MAC Address, IP Address, Clean Access Server, Description and Access Type fields are populated by 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 CAM displays this summary page, from the administrator's perspective, within the context of the CAM web interface. This allows easy access to endpoint location information, MAC and IP history, and a Layer 2 trace details – all displayed directly from within the CAM GUI, providing access to all contextual data gathered by NAC Profiler from a single unified interface. (Full information regarding endpoint summary views is provided in Chapter 13, "Using the Endpoint Console").

*Figure 11-5    Viewing NAC Profiler Endpoint Data from a CAM*
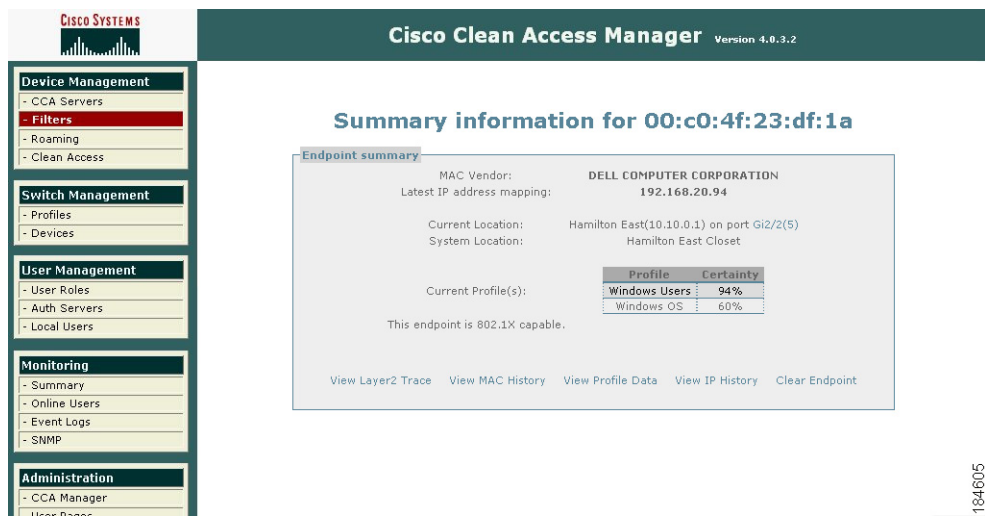


# View/Edit NAC Events List

To view the list of existing NAC Events on a NAC Profiler system, select the Configuration Tab from any page of the NAC Profiler web interface. Select NAC Profiler Events, and then select View/Edit NAC Events. A new page containing the Table of NAC Event Rules displays in the browser, as shown in Figure 11-6.

*Figure 11-6    Table of NAC Events*



The table provides a summary view of NAC Events currently saved to Cisco NAC Profiler configuration. Along with the name, the Profiles applicable to the NAC Event, the Access Type specified for Device Filter List entries made by the NAC Profiler NAC Event in the CAM, along with the current status of the

Event (enabled/disabled) are displayed for each NAC Event. Note that when a Regular Expression is specified in the NAC Event "Matches NAC Profiler Profile(s) field, the table of NAC Events displays the Regular Expression in the Profile column of the Table of NAC Events. In the example above for instance, the Regular expression /phone/i would result 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 CAM.

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 11-7.

*Figure 11-7        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 11-6 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.

Note      Selecting the Synchronize button prior to Save NAC Event will result in the changes to the NAC Event not being made. If changes to the NAC Event are made, select Save NAC Event to commit the changes to the database. To perform NAC Event-level synchronization, re-open the Save NAC Event and use the Synchronize button. Alternatively, perform a full synchronization by executing an Apply Changes -> Re-Model or Update Modules.

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 NAC Appliance Integration

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

- No barriers (e.g., firewalls or ACLs) to network communication between the NAC Profiler appliance running the Server module and the NAC Appliance CAM.

- Correct configuration of NAC Appliance CAM administrator web credentials in the NAC Profiler Server module (or other admin account with "full-control" API access).

- Correct configuration of SSH key-based authentication between the "profiler" user on Cisco NAC Profiler and the "root" user on the CAM.

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 NAC Profiler Server (console or SSH) and verify the following:

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

   ```
   $ ping <CAM-IP>
   $ traceroute –n <CAM-IP>
   ```

2. Data communication

   ```
   $ telnet <CAM-IP> 443
   ```
   Successful establishment of a telnet session is typically indicated by the following messages:

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

3. SSH key-based auth

   ```
   $ ssh root@<CAM-IP> ls /
   ```
   If ssh key-based authentication is functioning correctly then a directory from the CAM root directory will be shown, with no prompting for password

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 NAC Profiler and the CAM, or consider moving the systems onto the same network segment.

## Integration Debug Logs

From Cisco NAC Profiler (console or SSH) the system log may be examined for entries related to integration with NAC Appliance.   Such log entries will include the string "CCA_REQUEST" or "CCA_SYNC.   The following are typical commands that may be used for viewing these log entries:

- Show all related log messages to date

  ```
  # grep CCA_ /var/log/messages | less
  ```
- Watch related log messages as they happen

  ```
  # tail –f /var/log/messages | grep CCA_
  ```

Example log entries:

```
Jan  3 12:23:59 beacon CCA_REQUEST[28140]: [addmac 00:c0:b7:78:01:37] Success
Jan  3 12:24:01 beacon CCA_REQUEST[28168]: [addmac 00:c0:b7:66:82:b5] Success
Jan  3 12:24:02 beacon CCA_REQUEST[28169]: [addmac 00:c0:b7:67:3a:c7] Success
```

# Other Potential Issues

As was outlined early in the chapter, the integration between NAC Profiler and NAC Appliance is event-triggered. The integration actions of Add MAC and Remove MAC are triggered for a given endpoint upon it being Profiled into a Profile that matches a NAC Event (Add MAC), or changing from a Profile matching a NAC Event to another Profile that does not match a NAC Event (Remove MAC).

If an endpoint is already in a Profile matching one specified in a NAC Event when the integration is configured and applied, the Add MAC action is not triggered. Endpoints already in a Profile are not added to the Device Filter List because no event is triggered.