CHAPTER 10

Configuring NAC Profiler Events

This chapter includes the following topics:

Overview

Profiler Events are a critical component of the endpoint Behavior Monitoring capability of Cisco NAC Profiler as well as the integration with NAC Appliance. NAC Profiler is able to not only discover, locate and identify the endpoints on the network; it also constantly monitors the endpoint environment for changes. When the endpoint connected to a designated port changes, or if an endpoint begins exhibiting behavior indicating that the endpoint device type (e.g., Profile) has changed, these events are logged by the NAC Profiler and the system can automatically alert network operations or security management. In this way, the endpoint Behavior Monitoring function of Cisco NAC Profiler provides invaluable support for the ongoing management NAC Appliance deployments.

The Profiler Events functionality provides four event types: Newly Profiled, MAC Change, Profile Change, and NAC Events. The first three event types form the basis of the Behavior Monitoring alerting functionality. The fourth event type, the NAC Event, is used exclusively in the integration of NAC Profiler with NAC Appliance. This event type will be explored in detail in Chapter 11, "Integration with Cisco NAC Appliance," which outlines the process of configuring the integration between NAC Profiler and NAC Appliance.

Newly Profiled, MAC Change and Profile Change events are created and configured to alert network and security operations through one or a combination of common alerting mechanisms: SNMP traps to the NMS, Syslog entries on the NAC Profiler Server itself or another Syslog server on the network, as well as events notification within the Endpoint Console of the NAC Profiler web interface. Endpoint behavior monitoring can be utilized to assist in the ongoing management, troubleshooting and improvement of the network security posture by immediately and automatically alerting appropriate personnel and systems when changes of interest are occurring at the edge of the network.

The bulk of this chapter will describe the functionality of the three event types enumerated in the last paragraph, and how they are configured. NAC Events are covered in detail in Chapter 11, "Integration with Cisco NAC Appliance." Chapter 13, "Using the Endpoint Console," which outlines the use of the Endpoint Console, will describe how to view and manage Profiler Events through the NAC Profiler user interface.

Newly Profiled Event Type

This event is designed to alert when endpoints are first Profiled into one or more Profiles of interest. For example, it may be desirable to know when endpoints from a particular manufacturer are added to the network, possibly devices that are known to be unauthorized according to policy. As an example, assume that a Profile called 'Belkin Device' is designed to identify devices with a MAC Vendor of 'Belkin,' a known manufacturer of SOHO Access Point routers. As endpoints are discovered on the network and placed in the Belkin Device Profile, NAC Profiler can generate an event to notify that an endpoint has been added to this Profile, along with location information that could be used to generate a trouble ticket.

Newly Profiled Events are defined globally to a NAC Profiler system. When added to the system configuration, the event becomes enabled system-wide.

Profile Change Event Type

This event is used to alert when endpoints on designated ports transition from their steady-state Profile to another Profile. This event is enabled on selected ports at the network device level. Enabling of Profile Change events is configured per device using the Edit Network Device procedure outlined in Chapter 8, "Adding Network Devices to the NAC Profiler Configuration."

Note Profile Change events cannot be enabled on a network device until NAC Profiler has successfully polled the device via SNMP.

As is described in detail in Chapter 11, "Integration with Cisco NAC Appliance," when NAC Profiler is integrated with NAC Appliance an endpoint observed changing behavior warranting a Profile change from a Profile designated for inclusion on the Filter List of the CAM, to a Profile that is not designated (e.g., printer transitioning to Windows user, for example) may result in the entry for the endpoint being removed from the Filter List by NAC Profiler and the endpoint's current connection with the network terminated by NAC Appliance, depending on configuration. The Profile Change event can be utilized to alert network management that this action has occurred.

Note The event logic for Profile Change events is such that it does not log an event as a new, previously undiscovered endpoint joins the network on a port with Profile Change events enabled. In cases where a new endpoint joins and is initially Profiled into an enabled Profile, or is discovered and classified as Unknown, this sets the steady-state Profile for the endpoint for the purposes of this event type. If the new endpoint subsequently transitions from the steady-state Profile, to another Profile, or from Unknown to an enabled Profile, that transition away from the steady-state Profile to a new Profile will result in the Profile Change event being generated.

MAC Change Event Type

This event was designed to be used in environments where it is necessary to know when the MAC Address of the endpoints attached to designated ports on selected network devices change. An example might be ports that are not placed under the management of NAC Appliance. Endpoints connecting to these ports are not challenged for authentication credentials of any kind and are not postured. In effect there is no admission control applied to these ports. Therefore it is important to know if the MAC address

currently connected to that port changes. Like Profile Change events, MAC Change events are enabled on a per-port basis on selected network devices using the Edit Network Device procedure outlined in Chapter 8, "Adding Network Devices to the NAC Profiler Configuration."

Note MAC Change events cannot be enabled on a network device until NAC Profiler has successfully polled the device via SNMP.

MAC Change events are enabled on the ports at the network edge where a change to in the MAC address of the connected endpoint is of interest. MAC Change events should not be configured on trunk ports where multiple MAC addresses learned on the port is expected behavior. The model of the network maintained by NAC Profiler network tracks the network device (by MAC address) and port providing connectivity for each and every endpoint currently connected to the network. When a MAC Change event is enabled on an edge port, the NAC Profiler records the current MAC address connected to that port. The MAC Change event is triggered if and when a different MAC address is learned on that port indicating that the expected MAC has potentially been replaced,

Note If a MAC Change event is enabled on a port that is open (e.g., no endpoint connected), the first endpoint that connects to the port has its MAC address discovered by the NAC Profiler, but this does not trigger an event. Upon learning the first MAC address on a port enabled for MAC Change Events, the event becomes armed. If a new MAC address is learned by NAC Profiler on the port, the event is triggered and that MAC address becomes the reference MAC address for the port and if it changes, the event will fire again.

Note In the current implementation of MAC Change events, the event mechanism records only the last MAC to be learned on a port. Therefore in the case of an edge port supporting multiple devices through a fan-out device such as a hub, unmanaged switch or wireless access point, the MAC Change event does not provide a definitive indication of the previous MAC being removed from the port. Accordingly, these events should only be used on switch ports known to be supporting a single endpoint.

NAC Events

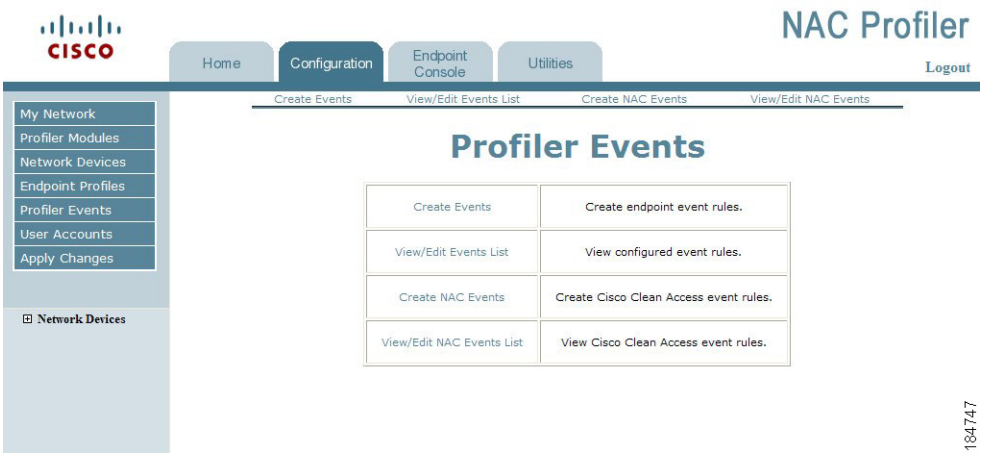
The NAC Profiler event capability is also used to provide necessary functionality to integrate with the Cisco NAC Appliance to significantly reduce the administrative burden of implementing and managing the network admission control solution from Cisco Systems. This integration of NAC Profiler with NAC Appliance provides automated population and management of the CAM Device Filter List. This list, which serves as a 'white list' of MAC addresses that cannot interact directly with NAC and should be admitted onto the network based on their MAC address. NAC Profiler integration in Cisco NAC Appliance deployments significantly reduces the administrative burden associated with accommodating non-NAC compliant endpoints, and can significantly improve the integrity of the network admission control mechanism by ensuring that the devices on the Filter List are constantly monitored for indications of potential attempts at unauthorized access.

Integration of the NAC Profiler with NAC Appliance, including the configuration of NAC events is covered in detail in Chapter 11, "Integration with Cisco NAC Appliance."

Configuring Profiler Events

To define Profiler Events select the Configuration tab and select Profiler Events from the left side bar or from the main pane table. Figure 10-1 shows the Profiler Events configuration page displayed in the browser.

Figure 10-1 Profiler Events Page

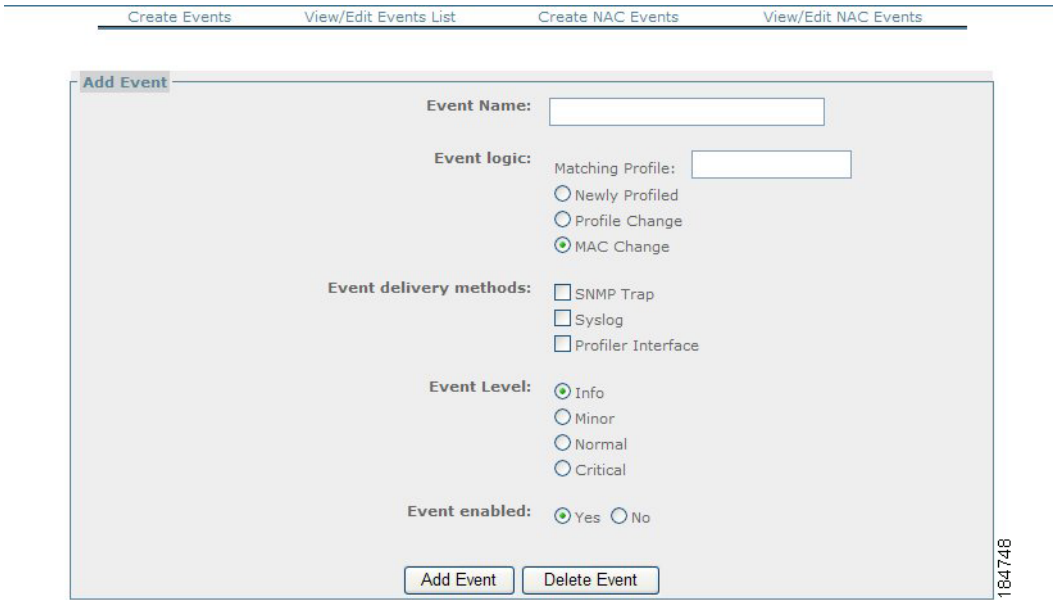


Create Profiler Events

Select the Create Events option from the table on the Profiler Events page (or the links at the top of the page) as shown in Figure 10-1 to create Newly Profiled, Profile Change or MAC Change events and add them to the system configuration.

The Add Event form is displayed in the main page as illustrated in Figure 10-2.

Figure 10-2 Add Event Form



To create a new endpoint event, complete the Add Event form for the desired event type using the instructions below.

Event Name

Enter a meaningful name to describe this particular event. When naming the event, consideration should be given to the fact that the Event Name is utilized in the configuration of Profile and MAC Change events on network devices. Accordingly, the name should be descriptive enough to ensure that they are recognizable when enabling events on selected devices.

Event Logic

Use the radio buttons to select the appropriate event type for the event being added: Newly Profiled, Profile Change or MAC Change.

Additionally, the Event Logic enables the administrator to select options to make the event mechanism more selective and hence enhancing the value of Profiler Events for the purposes of network operations and security management.

The **Matching Profile** field provides a mechanism to further refine the event by making the event mechanism more selective. Matching Profile will accept a regular expression that matches one or more Profile names.

For Newly Profiled events, the Matching Profile field is used to designate the Profile or Profiles that should be monitored for the addition of endpoints. In the example outlined earlier in the chapter, if it was desirable for NAC Profiler to generate an event each time an endpoint was added to the Profile named ‘Belkin Devices,’ the Matching Profile would have /Belkin/ entered in it.

For Profile Change events, the Matching Profiles field allows one or more Profiles to be designated as allowed Profile changes—that is transition from steady-state to the Matching Profile will **not** result in the event being generated. For example, if an endpoint transitioning from the Profile named ‘Cisco IP Phone (CP-7960G)’ to the Profile named ‘Cisco IP Phone CP-7970G’ was not a reason for alarm (IP phone upgrade), the regular expression /phone/i could be entered in the Matching Profile field signifying that such a Profile change was allowable and not worthy of an event.

For MAC Change events, the Matching Profiles field is optional and allows one or more Profiles to be designated as allowable MAC changes—that is if a MAC in a Profile with a name matching what is specified in the Matching Profiles field were to be replaced with another device (different MAC) that was also in a Profile with a name matching what is specified in the Matching Profiles field, **no** MAC Change event would result. For example, if endpoint with MAC A which was currently in the Profile named 'Printer' was replaced with MAC B which was also in the Printer Profile on a port with a MAC Change event enabled and the Matching Profile field set to /Printer/, no MAC Change event would be generated by this endpoint replacement.

Event Delivery Methods

NAC Profiler provides four Endpoint Event delivery methods applicable to Newly Profiled, Profile Change and MAC Change events. Those delivery methods are as follows:

- SNMP Trap – NAC Profiler will issues an SNMP Trap to the SNMP Manager IP Address defined in the Server Module Configuration window.
- Syslog – NAC Profiler will write a syslog message based on the settings in /etc/syslog.conf.
- NAC Profiler Interface – NAC Profiler will display the event in the Profiler Events page of the Endpoint Console provided by the user interface.

Any combination of the three options can be selected for the Endpoint Event being created.

Event Level

Select one of the four available Event Level options (Info, Minor, Normal or Critical) to aid operators in the interpretation of the priority/severity of this Endpoint Event.

Event Enabled

Once defined the Event can be enabled or disabled at any time by selecting the appropriate option.

Select the Add Event button to save the newly created Endpoint Event.

If additional Profiler Events are desired, repeat the process outlined in this section to create the Newly Profiled, Profile Change and MAC Change events required. When all desired events have been added to the system configuration, move onto enabling Profile Change and MAC Change events on selected ports of selected network devices as described in the next section.

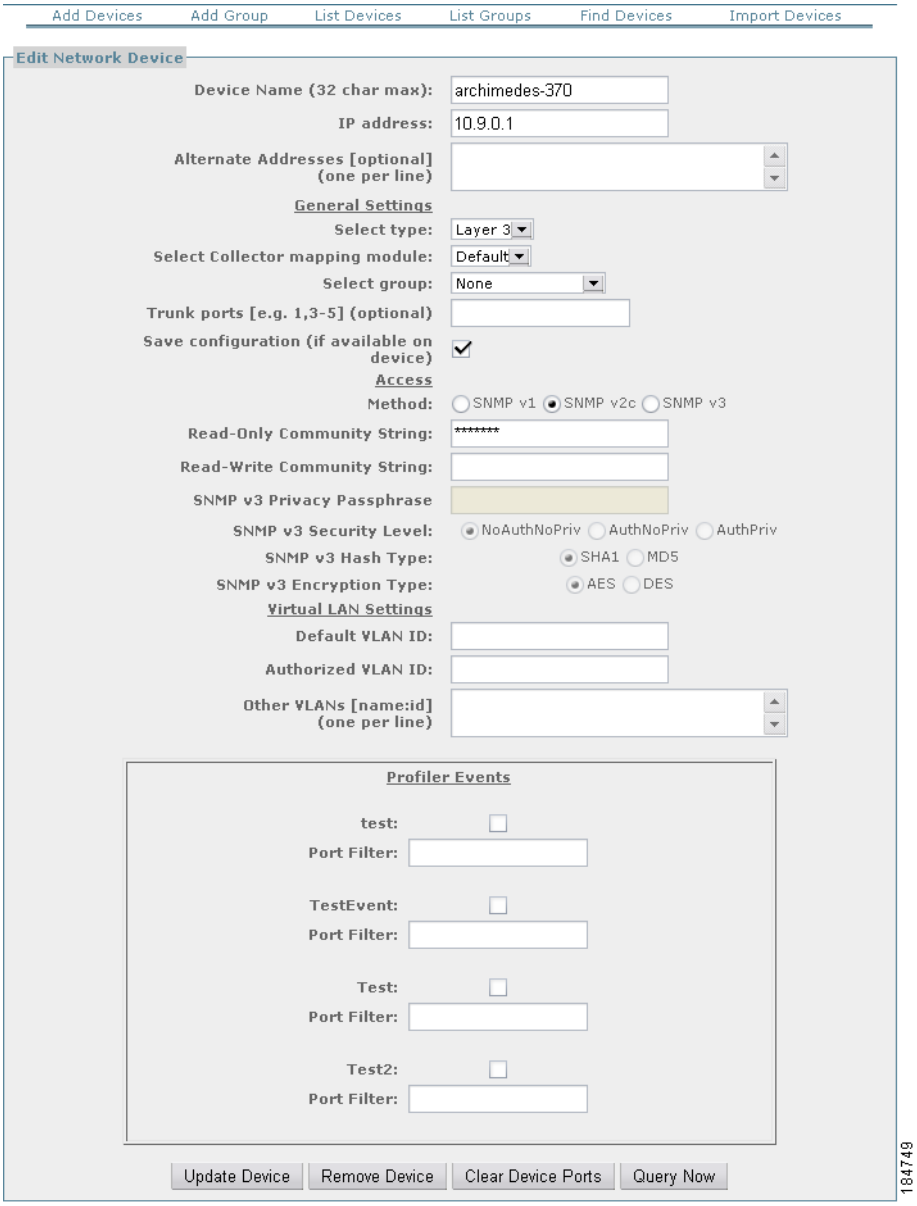
Enable Events per Network Device

Note Newly Profiled events are enabled globally and do not require enabling on network devices. For Newly Profiled events, skip this section and proceed to the next section of this chapter.

As mentioned earlier in the chapter, Profile Change Events and MAC Change Events are enabled on selected network devices on a per-port level. In order for Profile Change and MAC Change events that have been defined as described above to be activated, they must be enabled on the network devices at the edge of the network on ports of interest.

If Profile Change or MAC Change Events have been added to Cisco NAC Profiler configuration, and after a network device is polled via SNMP for the first time, a new section entitled "Profiler Events" is added to the Edit Network Device form as shown in Figure 10-3. (For a full guide to network device configuration in NAC Profiler, refer back to Chapter 8, "Adding Network Devices to the NAC Profiler Configuration.") This section allows for each network device in the configuration to have any of the Profile Change or MAC Change events saved to the system configuration enabled on selected ports.

Figure 10-3 Edit Network Device Form—Profiler Events



As illustrated in Figure 10-3, after a network device has been polled successfully by NAC Profiler, the available Profile Change and MAC Change Events can be enabled on the device. The Profiler Events section of the Edit Network Device form will have two items for each Profile Change and/or MAC Change event in the system configuration as shown in Figure 10-3.

To enable a MAC Change or Profile Change event on a network device, simply select the checkbox adjacent to the event name. This enables the event on all ports. The Port Filter field allows designation of port or ports to **exclude** from the event checking process. Ports that should not be enabled/checked for events, such as inter-switch links in the case of MAC Change events for example, should be added to the Port Filter list.

Note The syntax for the Port Filter list is the ifIndex of the port(s) to be excluded from event enablement. Individual ports can be specified separated by commas (e.g., 1,5,11, etc.) and or ranges of ifIndices (e.g., 1-5,7,8, etc.)

Once the desired parameters have been entered on the Edit Network Device form, select the Update Device button. Complete the configuration on all remaining network devices that will have either Profile Change or MAC Change events created in the last step enabled on their respective ports as outlined above. When complete, proceed to the next section which outlines how to make the configured Profiler Events active on Cisco NAC Profiler.

Activating Profiler Events

In order for Profiler Events to become active, the configuration changes outlined in earlier sections need to be committed to the running configuration of the system.

In the case of Newly Profiled events, as soon as the event is created and saved, execute an Apply Changes -> Update Modules. After execution of the Update Modules, each time an endpoint is profiled into any Profile with a Profile Name that matches the Matching Profile entry in the Newly Profiled event, the event will be triggered.

Note For the Newly Profiled event, if endpoints were currently in the Profile(s) specified in the Matching Profiles entry for the event prior to the activation of the event, the event will not be triggered for these endpoints as the event logic requires that an endpoint be added to the Profile post event activation. To force the event to occur for endpoints in a Profile prior to Newly Profiled event activation, temporarily disable the Profile, perform an Apply Changes -> Update modules, and then re-enable the Profile. This action will result in the Profile being purged and endpoints being re-Profiled which will trigger the event for the endpoint(s).

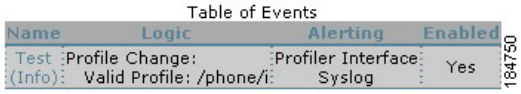
For Profile Change and MAC Change events, after the enablement of the event on the desired Network Devices, execute an Apply Changes -> Update Modules. After execution of the Update Modules, the Profile Change and or MAC Change event or events are effectively activated on the network devices and ports as configured in the step above.

If configured correctly, when a Profile Change, MAC Change or Newly Profiled event occurs, the notification(s) specified in the respective event configuration should show the event. For a description of NAC Profiler's Event display and management provided within the Endpoint Console, please see Chapter 13, "Using the Endpoint Console."

Edit Profiler Events

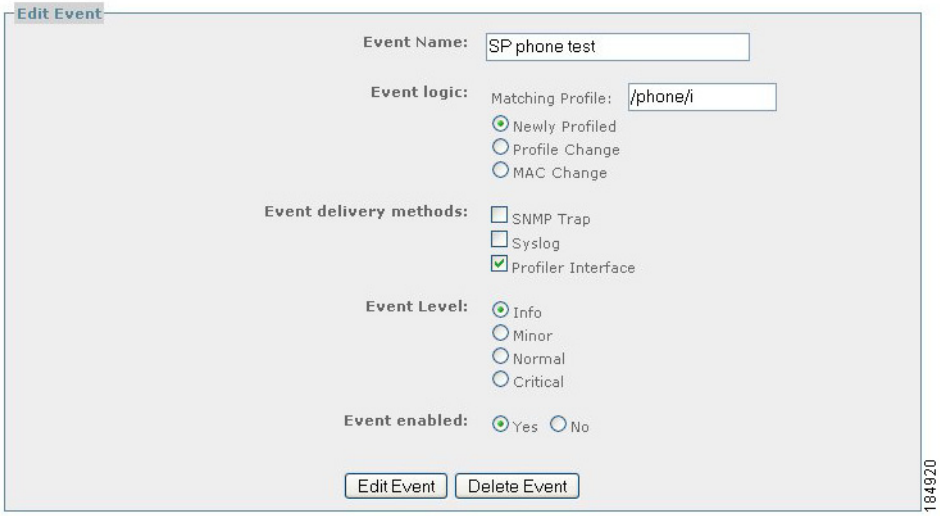
To view the list of Profiler Events saved on the system and their current status select the View/Edit Events List link in the Profiler Events table. Figure 10-4 is an example of the table that will be presented upon selecting View/Edit Events:

Figure 10-4 Table of Events



Selecting the green hyperlinked Event Name will open the Edit Event form shown in Figure 10-5.

Figure 10-5 Edit Event Form



The form is populated with the current event parameters which can be edited as desired. Refer to the section of this chapter entitled Create Profiler Events for a description of each parameter and instructions for defining a Profiler Event.

Temporary enablement or disablement of the Endpoint Event can be accomplished by selecting the appropriate radio button.

After making changes to the event that are to be committed to the system, be sure to select the Save Event button to save the changes to the system configuration.

If the event is to be deleted, select the Delete Event button to remove the event from the system configuration.

Note Remember that Profile Change and MAC Change events are configured on selected network devices on designated ports. If there are changes to be made to these types of Profiler events on a device and/or port level, those changes must be made to the effected network device configuration as described in this chapter.

After desired changes are made, the changes must be committed to the running system configuration. Execute an Apply Changes -> Update Modules to commit the edits to Profiler Events.