CHAPTER 7

Add Support for New Events

The VCB can be used to enable Prime Network to recognize additional events and to customize the way events are handled. For example, you might want Prime Network to recognize traps that are specific to a new technology or a custom syslog that you have defined. You might also want to change the settings of a system default event, for example, change the severity from major to minor.

You can customize events using the VCB tool within Prime Network, or using VCB CLI commands. This chapter describes event customization using the Prime Network VCB GUI. For information on using the CLI method, see CLI Commands for Adding and Customizing Events, page C-32.

These topics explain how to use the VCB to create support for events, and to change how events are handled:

- Enable Support for Unsupported Traps, page 7-1
- Enable Support for a Custom Syslog, page 7-6
- Customize Events, page 7-9

For general information about the VCB, see VCB Overview, page 3-1. For information on the level of support for various features in the different types of VNEs, see Comparing Generic SNMP VNEs, U-VNEs, and Developed VNEs, page 3-3.

Enable Support for Unsupported Traps

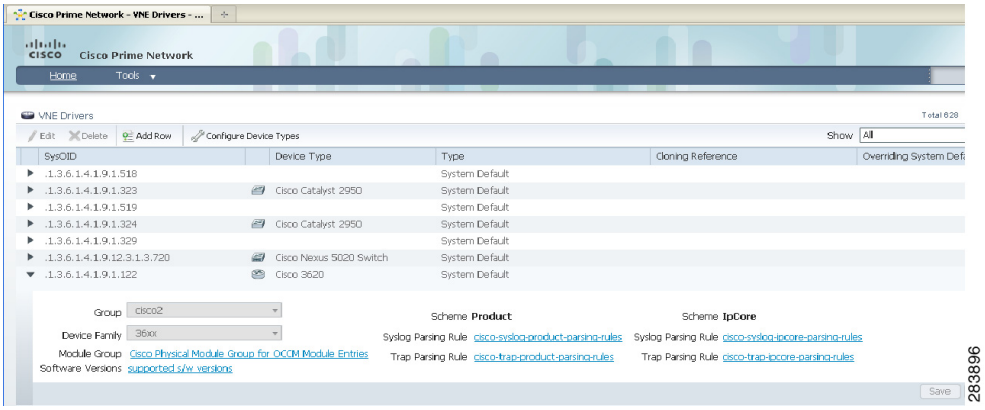
This procedure describes how to add unsupported traps as events in Prime Network based on a particular MIB definition file.

Use the VCB to add support for unsupported traps, as follows:

Step 1 In the VCB tool, go to the VNE Drivers tab.

Step 2 Click on the arrow next to the VNE driver on which you want the additional traps to be supported.

Figure 7-1 Expanded VNE Driver Properties Showing Parsing Rules



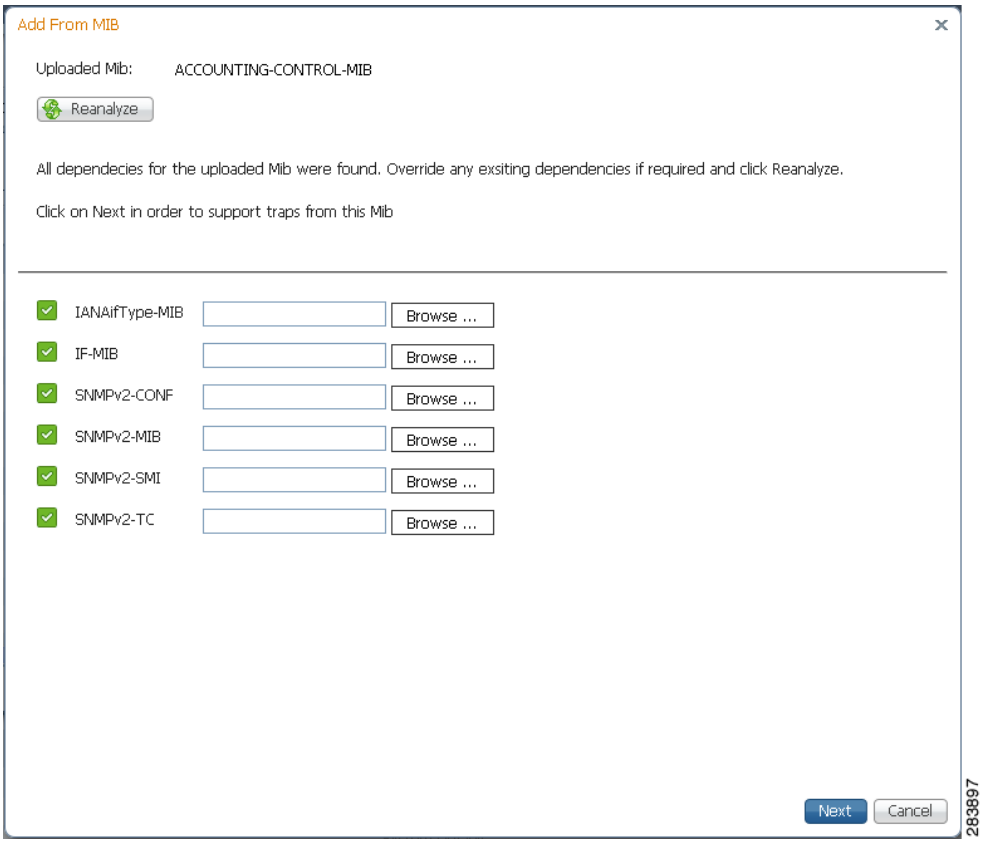
Step 3 Click the Trap Parsing Rule link to show a list of traps associated with this parsing rule.

Step 4 Click **Add from MIB**. This launches a wizard which enables you to analyze a specified MIB and select the traps to be supported.

Step 5 Click **Browse** and select the MIB file you want to upload to the Prime Network gateway. You can upload an individual MIB file or a zip file containing multiple MIB files. The file extension should be .mib or .my, .zip, or no extension. If you select a zip file, a list of the contained MIBs is displayed. You can select one or more of these MIBs to upload.

A list of MIB dependencies is displayed. A green check mark indicates that the dependency file has been found on the server.

Figure 7-2 MIB Dependencies



Step 6 If any of the dependencies is not found, click **Browse** and select the dependency file to upload.

Step 7 Click **Next**. A list of traps is displayed. A red icon to the left of the trap indicates that it is not supported. A green icon indicates that the trap is already supported.

Step 8 Check the check box next to the trap(s) to be supported. If you select multiple traps, they must be of the same type. Click **Next**.

At this point, an event is created. Each trap you selected becomes a sub-type of the new event. The Event Definition wizard is displayed to enable you to complete the definition of the new event.

Step 9 Click on **Step 1 - Event Definition** and provide the following information:

- Event name and OID—these are pre-populated but can be changed if necessary. The OID is the common prefix of the OIDs of the selected subtypes.
- Category—predefined category from 3GPP standards (according to ITU-T Recommendations X.733 and X.736). You can change the category if necessary.
- Nature—defines whether the event is automatically cleared by a clearing event or it needs to be manually cleared. Possible values are:
  - ADAC (Automatically Detected Automatically Cleared)—The event is automatically detected and automatically cleared by the system. For example, “link down” event. Select this option if the event has a clearing event, for example, “link up”.
  - ADMC (Automatically Detected Manually Cleared)—The event must be manually cleared by the user. For example, "DWDM fatal error" syslog. Select this option if the event does not have a clearing event.

Step 10 Click on **Step 2 - Subtype Definition**. You will see that a subtype has been created for each unsupported trap you selected. Edit the information for each subtype as required:

Field	Description
Name	Enter a unique name for the event subtype
Description	Enter a string that describes the event subtype.
Severity	Select the severity to be attributed to the subtype.
Ticketable	Check the check box if you want Prime Network to create a ticket for this event if there is no root cause event to which it can be correlated. If you make a sub-type ticketable, a ticket will be generated for it. When a non-ticketable sub-type of the same event arrives (for example, a warning or clearing event), the ticket will be updated.
Auto-Clear	Check the check box if you want Prime Network to automatically clear the event. Prime Network clears a ticket if all of its events either are cleared or are configured for automatic clearing.
Correlate	Check the check box if you want the event to be correlated to a root-cause alarm.

Step 11 Click on **Step 3 - Subtype Identification**. In this step, you define how Prime Network will differentiate between the subtypes, as follows:

Field	Description
By TrapOID	Select this option if each subtype has a unique OID. In the Replacing Rules section, specify the OID suffix for each subtype. The OID suffix must be an integer.
By Varbind Value	Select this option if the subtypes have the same trap OID and you want to use one of the varbind values to differentiate between the subtypes. In the Replacing Rules section, select the required varbind from the drop-down menu or enter free text, and then define the values for each subtype.
By Varbind OID	Select this option if there is a varbind for each subtype. In the Replacing Rules section, specify the common prefix of the varbind OIDs and the suffix for each subtype.

Step 12 Click on **Step 4 - Association**, in which you associate the event with the VNE. Specify the following information:

Field	Description	
Source Type	The entity to which the event should be associated.	
	ManagedElement Key	Select this option if there is no specific interface or other component of the VNE from which the event is generated.
	Efp Key From Ifname Serviceid	Associates the event with a specific EFP DC, based on the service instance ID and the interface name.
	Interface Key From Ifindex	Creates the interface device component key from the ifIndex and associates the event with the appropriate interface layer.
	Interface Key From Ifname	Associates the event with a specific interface that you specify in the Interface Identifier field.
	Logical Container Key	Associates the event with a designated logical container that you select in the Logical Container field.
	ModuleDC Key Given EntPhysicalIndex	Associates the event with a designated module DC.
	ModuleDC With SlotSubslot Value Key	Associates the event with the corresponding module, based on the slot number.
	Pw Interface Key From Tunnelindex	Associates trap events with the designated pseudowire tunnel interface.
Logical Container	Applicable only when the source type is Logical Container Key. This field lists the various logical containers for which the VCB supports event association. For example, BGP traps/syslogs can be associated with the MP-BGP type container, ISIS events with the ISIS System container, and so on.	
Instance Identifier Location	Specify whether the identifier of the event is based on a value or a varbind OID.	
Instance Identifier Varbind OID	Select the varbind that contains the instance information. Prime Network uses varbind OID to locate the varbind in the trap PDU and locates the instance information from either the OID or the value depending what was selected as the instance identifier location (OID or value).	
Source Location	Specify whether the event source can be found in a value or a varbind OID	
Source Varbind ID	Select the varbind that contains the source information. Prime Network uses varbind OID to locate the varbind in the trap PDU and locates the source information from either the OID or the value depending what was selected as the source location (OID or value).	

Step 13 Click on **Step 5 - Pattern** to determine which VNE drivers will be extended to support this event. This is determined by selecting the parsing rule groups per scheme that will be extended. The event will be supported on all VNE drivers that use the specified parsing rule groups.

Step 14 Click **Add** to select additional parsing rule groups, as required, either for the Product or IpCore scheme.

Note Certain parsing rules groups inherit from other groups. If you select multiple groups, make sure that your selection does not include a base (parent) group as well as the group that inherits from the base group. See Parsing Rule Group Inheritance Structure, page 7-9 for the relationship between parsing rule groups.

Step 15 Click **Finish**. A dialog box displays a list of the traps that were added.

Step 16 If you want to enable support for additional traps, click **Select Different Trap**, otherwise click **Close**.

Enable Support for a Custom Syslog

In this example, a custom syslog is generated by a router, using Embedded Event Manager (EEM), when the Windows XP server being monitored is not reachable. The custom syslog is %HA_EM-6-LOG: IPSLA-XP: Windows-XP unreachable. This event is sent to Prime Network but is not recognized or parsed.

Use the VCB to add support for this custom syslog, as follows:

Step 1 In the VCB tool, go to the VNE Drivers tab.

Step 2 Click on the arrow next to the VNE driver that represents the router that generates the custom syslog to expand its display. The Syslog Parsing Rule field shows the parsing rule used to parse events for this VNE driver, for both Product and IpCore schemes.

Step 3 Click the Syslog Parsing Rule link to show a list of syslog events associated with this parsing rule.

Step 4 Click the Add Row button to start defining the new syslog.

Step 5 Enter a unique name for the syslog in the Event Name field. For example, Monitoring XP Server.

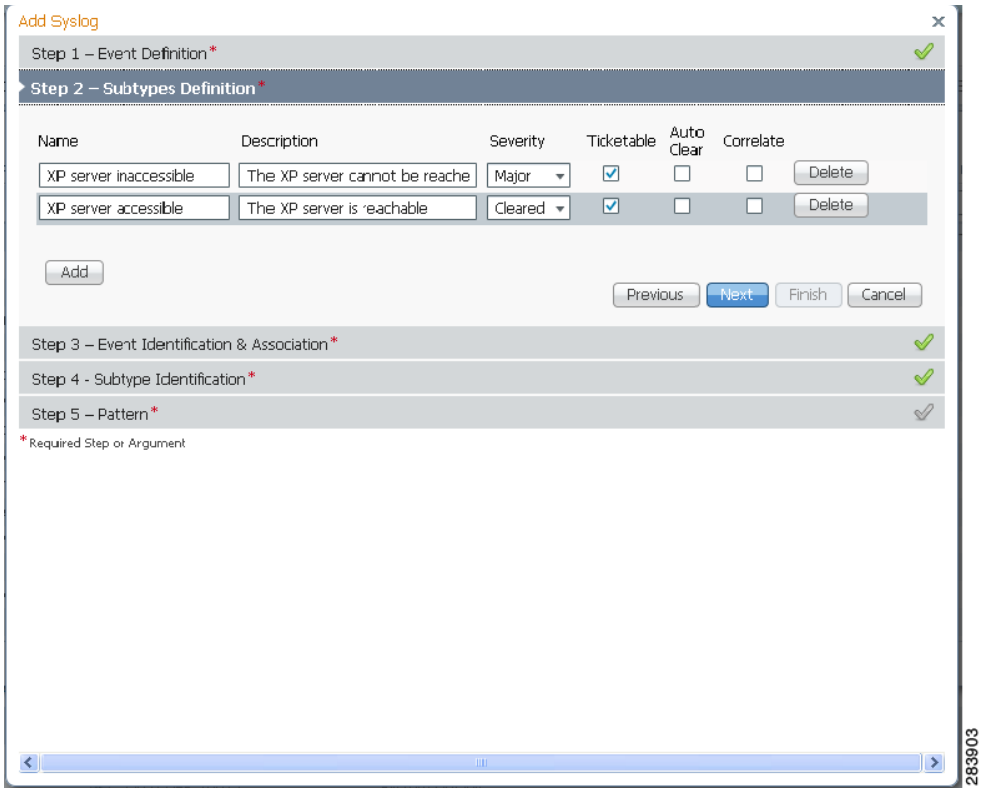
Step 6 Click **Next** to go to the next step in the wizard which is to define the event subtypes.

Step 7 Enter the following information to define the first event subtype:

Field	Description
Name	Enter a unique name for the event subtype, for example, XP server inaccessible.
Description	Enter a string that describes the event, for example, “The XP server cannot be reached.”
Severity	Select the severity to be attributed to the event.
Ticketable	Check the check box if you want Prime Network to create a ticket for this event if there is no root cause event to which it can be correlated.
Auto Clear	Check the check box if you want Prime Network to automatically clear the event, without waiting for a clear event or for manual clearing of the event. If the auto clear check box is checked, the event will be cleared automatically 4 minutes after the last modification.
Correlate	Check the check box if you want the event to be correlated to a root-cause alarm.

Step 8 Click **Add** to define a second subtype, for example, XP server accessible, with severity “Cleared”.

Figure 7-3 Subtype Definition



Step 9 Click **Next** to go to the next step in the wizard which is identification and association of the event. In this step, you will provide an example of the raw event and you will define parameters by which the event will be identified.

Step 10 Enter the following information to define event identification and association.

Note You can provide multi-word values for the following parameters in the Event Identification and Association section while creating a syslog event: Interface Identifier, Interface Name, Substring(s) to Ignore, Subtype Key, and Instance Identifier Prefix.

Field	Description
Raw Event	Provide the raw event syntax as an example, so that the system can parse it.
Subtype Key	Keyword that identifies the subtype. The keyword should be taken from the raw event. In this example, the key would be “unreachable”.

Field	Description	
Source Type	Select the source component of the device from which the event is generated. For this example, select ManagedElement Key because there is no specific interface or other component from which the event is generated. In other cases, you might choose from the following options:	
	Efp Key From Ifname Serviceid	Associates the event with a specific EFP DC, based on the service instance ID and the interface name.
	Interface Key From Ifname	Associates the event with a specific interface that you specify in the Interface Identifier field.
	Logical Container Key	Associates the event with a designated logical container that you select in the Logical Container field.
	ModuleDC With SlotSubslot Value Key	Associates the event with the corresponding module, based on the slot number.
Instance Identifier Prefix	The unique identifier prefix that you specify in the new event location string which helps you to differentiate between the same event on the same interface but with a different CLI. The instance identifier prefix you provide will be displayed in Cisco Prime Network Vision and Cisco Prime Network Events along with the location identifier.	
Logical Container	Applicable only when the source type is Logical Container Key. This field lists the various logical containers for which the VCB supports event association. For example, BGP traps/syslogs can be associated with the MP-BGP type container, ISIS events with the ISIS System container, and so on.	
Interface Identifier	Specify a value by which the interface will be identified (ifIndex is used to identify the interface).	
Interface Name	Specify the name of the interface to which the event is associated ((ifName is used to identify the interface).	
Instance Identifier	Specify the identifier of the instance. For this example, the instance identifier could be Windows XP.	
Substring(s) to Ignore	Prime Network filters the events that need to be parsed and processed based on the value(s) specified in this argument.	

Step 11 Click **Next** to go to the next step in the wizard which is identification of the event subtypes. In this step, you will define values for each of the subtypes. In this example, the values could be “unreachable” for XP server inaccessible and “reachable” for XP server accessible.

Step 12 Click **Next** to go to the next step in the wizard which determines which VNE drivers will be extended to support this event. This is determined by selecting the parsing rule groups per scheme that will be extended. The event will be supported on all VNE drivers that use the specified parsing rule groups.

Step 13 Click **Add** to select additional parsing rule groups, as required. In this example, all VNE drivers associated with group cisco-syslog-product-parsing-rules will be extended to support the new syslog. You can select additional groups for the Product scheme or you can select the IpCore scheme and a parsing rule group.

Note Certain parsing rules groups inherit from other groups. If you select multiple groups, make sure that your selection does not include a base (parent) group as well as the group that inherits from the base group. See Parsing Rule Group Inheritance Structure, page 7-9 for the relationship between parsing rule groups.

Step 14 Click **Finish**. The event now appears in the list of syslogs for the cisco-syslog-product-parsing-rules group.

Parsing Rule Group Inheritance Structure

Table 7-1 shows the inheritance structure for parsing rule groups. The groups on the left inherit settings from the groups on the right.

Table 7-1 Parsing Rule Groups Inheritance

This Parsing Rule Group...	Inherits Settings from This Group:
cisco-asr90xx-syslog-ipcore-parsing-rules	cisco-iox-syslog-ipcore-parsing-rules[1]
cisco-asr90xx-trap-ipcore-parsing-rules	cisco-iox-trap-ipcore-parsing-rules
cisco-ciscocpt-trap-ipcore-parsing-rules	cisco-trap-ipcore-parsing-rules
cisco-ciscocpt-trap-product-parsing-rules	cisco-trap-product-parsing-rules
cisco-iox-syslog-ipcore-parsing-rules	cisco-iox-syslog-product-parsing-rules
cisco-syslog-ipcore-parsing-rules	cisco-syslog-product-parsing-rules
cisco-trap-ipcore-parsing-rules	cisco-trap-product-parsing-rules
nexus-trap-product-parsing-rules	nexus-422v-trap-product-parsing-rules

1. Multiple inheritance levels: cisco-iox-syslog-ipcore-parsing-rules inherits from cisco-iox-syslog-product-parsing-rules. Therefore, if cisco-iox-syslog-product-parsing-rules is selected, do not select cisco-asr90xx-syslog-ipcore-parsing-rules and cisco-iox-syslog-ipcore-parsing-rules.

Customize Events

Using the VCB, you can change the way Prime Network deals with events. For example, you can change the severity of an event, or you can instruct the system to drop the event. Event customization is described in the following sections:

- Change the Severity of an Event Subtype, page 7-9
- Drop an Event, page 7-10
- Restore a System Default Event, page 7-10
- Delete Events, page 7-11

Change the Severity of an Event Subtype

The events that are supported by default in Prime Network are attributed with a specific severity. You can customize the event and change the severity if it is not appropriate for your organization. For example, the Prime Network system considers the event, “ASR5 port down” to have a severity of “Warning”. However, in your organization, this event might be considered to be “Major” and you want the event to be marked as such.

To change the severity of an event subtype:

Step 1 In the VCB tool, select **Tools > Events** or click on the Events tab.

Step 2 Click the arrow next to the event you want to customize to expand its display.

Step 3 Select the required severity from the Severity drop-down menu and click **Save**.

Drop an Event

By default, when an event is received by Prime Network, it is archived and parsed. Only events that have been parsed will appear in Prime Network Events tables. You can choose to drop an event so that it no longer appears in the tables. The event will no longer be actionable, meaning that it will not be processed and parsed, but it will be archived. In the case of service events, the event will no longer be generated by the system so there will be no archiving.

To drop an event:

Step 1 In the VCB tool, select **Tools > Events** or click on the Events tab.

Step 2 Select the event you want to drop and click **Modify Inbound Handling**.

Step 3 Click **OK** in the confirmation message.

The Inbound Handling column for the event will change to Archived Only for syslogs and traps or to Disabled for system events.

Restore a Dropped Event

To restore a dropped event:

Step 1 In the VCB tool, select **Tools > Events** or click on the Events tab.

Step 2 Select the event you want to drop and click **Modify Inbound Handling**.

Step 3 Click **OK** in the confirmation message.

The Inbound Handling column for the event will change to Archived Only for syslogs and traps or to Disabled for system events.

Restore a System Default Event

If you have edited a system default event and you want to go back to the original event, you can restore the system default event.

The Overriding System Default column indicates whether or not a system default event has been edited. The values for this column are true or false.

Note A VNE upgrade package might provide support for events that you previously added using the VCB. After you have upgraded the VNE driver, such events are marked as overriding the system default. Use this procedure to restore the system default event that is provided with the upgrade.

To restore a system default event:

Step 1 In the VCB tool, select **Tools > Events** or click on the Events tab.

Step 2 Select the event you want to restore and click **Restore**.

Step 3 Click **OK** in the confirmation message.

The Overriding System Default column for the event will change to False.

Delete Events

User-defined events can be deleted as long as they are not overrides of system default events. System default events cannot be deleted.

Note For system default overrides, a Restore button is provided instead of the Delete button.

To delete an event:

Step 1 In the VCB tool, select **Tools > Events** or click on the Events tab.

Step 2 Select the event you want to delete and click **Delete**.

Step 3 Click **OK** in the confirmation message.

The event is removed from the table.