Configuring Devices

These topics describe the configuration tasks you must perform so that Prime Network can properly model and manage your network.

Note Prime Network automatically performs a series of validation checks for Cisco IOS XR devices. See Cisco IOS XR Devices—Required and Recommended Settings, page A-3.

- Choosing a VNE Scheme (Check Technologies and Device Types), page A-2
- Why Device Configuration Tasks Are Important, page A-2
- Cisco IOS, Cisco IOS XE, and CatOS Devices—Required Settings, page A-3
- Cisco IOS XR Devices—Required and Recommended Settings, page A-3
- Cisco StarOS Devices—Required Settings, page A-6
- Cisco Nexus OS Devices—Required Settings, page A-7
- Cisco Carrier Packet Transport Devices—Required Settings, page A-9
- Cisco Unified Computing System Devices—Required Settings, page A-10
- Cisco ME 1200 Devices—Required Settings, page A-11
- All Cisco Devices Added Using SSH—Required, Recommended, and Rollback Device Settings, page A-11
- SNMP Traps and Informs—Required Device Settings, page A-12
- Syslogs—Required Device Settings, page A-17
- IP Address Configuration for Traps, Syslogs, and VNEs, page A-18
- TACACS, TACACS+, RADIUS Integration - Required Device Settings, page A-19

Choosing a VNE Scheme (Check Technologies and Device Types)

VNE schemes determine what data should be retrieved for each device, and which commands and protocols Prime Network should use to collect that data. Prime Network provides three schemes by default

Scheme	Use this scheme for:
Product	For devices that are not part of the network core, such as the Cisco 800 Series or 2900 Series.
IpCore	For devices that are part of the network core, such as the Cisco 3600 Series or CRS (Carrier Routing System) Series.
EMS	For devices where only system information and physical inventory should be polled (that is, the minimum amount of data). It is supported on all devices but does not support any technologies.
Default	For cases where you are not sure which scheme to choose. Prime Network will use the Product scheme.

While all Cisco devices support either the Product or IpCore scheme, most devices support both schemes but with different levels of support. Refer to the *Cisco Prime Network 4.3.2 Supported Technologies and Topologies* for information on:

- Which scheme to use depending on the technologies used on your network
- Whether a device type supports the Product and (or) IpCore schemes

You can also create your own scheme and it will be added to the Administration GUI client so you can apply it to VNEs. See Creating a Custom VNE Scheme, page 4-11.

Why Device Configuration Tasks Are Important

Prime Network VNEs communicate with network devices using a variety of protocols such as SNMP, Telnet, and ICMP. When a VNE is created, Prime Network connects to the device and runs a variety of registration commands to build a model of the device, based on the scheme that is chosen for the VNE. After modeling, ongoing notifications and protocol communication allows Prime Network to perform ongoing service and technology monitoring, fault processing, topological and model updates, and so forth. If the required device settings are not configured properly, Prime Network cannot retrieve the necessary information from the network element.

For example, if a new interface is added to a Cisco IOS device, but the **logging enabled** command is not set, Prime Network will not receive a device config change syslog from the device. As a result, Prime Network's copy of the startup device configuration file is outdated. If the device goes down, when it is restarted, the configuration change is lost.

Note Do not change the device's default packet size (which 1500 bytes). SNMP requests are sent in bulk by default. A small packet size could result in truncated responses.

Cisco IOS, Cisco IOS XE, and CatOS Devices—Required Settings

The following settings are *required* for Cisco IOS, Cisco IOS XE, and Cat OS network elements:

```
snmp-server community public-cmty RO
snmp-server community private-cmty RW
```

This settings is required for Cisco IOS and Cisco OS XE devices (it is already set by default for CatOS devices):

```
snmp-server ifindex persist
```

Do not change the device's default packet size (which 1500 bytes). SNMP requests are sent in bulk by default. A small packet size could result in truncated responses.

This setting disables domain lookups (which can cause Telnet command delays):

```
no ip domain-lookup
```

Reduced Polling

Reduced polling is supported on all Cisco IOS, Cisco IOS XE, and CatOS devices. These device types also support failsafe mechanism.

For Cisco IOS devices using reduced polling, the following settings are required.

```
configure terminal
archive
log config
logging enable
```

If a device is generating configuration change events but Prime Network is not recognizing them, edit the VNE properties (Events tab) and add the IP address you want the VNE to listen to. See VNE Properties: Events, page D-17.

Cisco IOS XR Devices—Required and Recommended Settings

Prime Network validates the configuration of Cisco IOS XR devices before creating VNEs for those devices. The validations are contained in a registration named **mis-con**, which validates the following:

- The MGBL package is installed.
- The user belongs to **root-system**.
- XML is enabled on the device. See Enabling XML on a Device, page A-4.

If any of these validations fail, Prime Network generates a System event. To disable this validation for all Cisco IOS XR devices, use the following command from the gateway server:

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/cisco-router-iox-ipcore-scheme/com.sheer.metrocentral.coretech.common.dc.ManagedE
lement/mis-con/enable" false
success
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/cisco-router-iox-product-scheme/com.sheer.metrocentral.coretech.common.dc.Managed
Element/mis-con/enable" false
success
```

The following settings (not included in the validation check) are *required* for Cisco IOS XR network elements:

Note If applicable, be sure to commit **snmp-server *community*** before **snmp-server *host***.

```
domain ipv4 host gateway_name gateway_IP
telnet ipv4 server max-servers no-limit
snmp-server community community_name SystemOwner
snmp-server community community_name RO
snmp-server entityindex persist
snmp-server ifindex persist
vty-pool default 0 99
xml agent tty
```

To include the location of an event for an IOS XR device, execute the following command:

```
# logging events display-location
```

This setting disables domain lookups (which can cause Telnet command delays):

```
domain lookup disable
```

Enabling XML on a Device

There are three different methods for XML communication between devices and Prime Network. The device configuration required depends on the method you are using.

- TTY XML Agent—To enable a TTY XML agent on a device, use the following commands. (In this case you do not need to enter any information in the VNE's XML tab in the Administration GUI client).

  ```
  configure terminal
  xml agent tty
  commit
  ```

- Dedicated XML agent—With a dedicated XML agent on the router, incoming XML sessions are handled over the dedicated TCP port 38751. In the Administration GUI client, enable XML on the VNE using the Telnet protocol. Enter the following commands on the device:

  ```
  configure
  xml agent
  aaa authorization exec default local
  commit
  exit
  ```

- SSL XML agent—With a dedicated SSL agent on the router, incoming XML sessions are handled over the dedicated TCP port 38752. In the Administration GUI client, enable XML on the VNE using the SSL protocol. Enter the following commands on the device:

  ```
  configure
  xml agent ssl
  aaa authorization exec default local
  commit
  exit
  ```

Reduced Polling

Reduced polling is supported on all Cisco IOS XR devices. This device type also supports failsafe mechanism. For Cisco IOS XR devices using reduced polling, the archive must be enabled (it is enabled by default).

If a device is generating configuration change events but Prime Network is not recognizing them, edit the VNE properties (Events tab) and add the IP address you want the VNE to listen to. See VNE Properties: Events, page D-17.

Other Guidelines for Cisco IOS XR Devices

Do not change the device's default packet size (which 1500 MB). SNMP requests are sent in bulk by default. A small packet size could result in truncated responses.

In addition to the required settings, you must follow these guidelines:

- Install the Cisco IOS XR Manageability Package (MGBL) on top of the Cisco IOS XR version. You can get information on this package from the release notes for your Cisco IOS XR version. (Prime Network automatically performs a validation check to ensure the MGBL package is installed.)
- Prime Network should use the device login user that is a member of group **root-system** and **cisco-support**. (Prime Network automatically performs a validation check to ensure this is properly configured.)
- To correctly model logical routers, the Prime Network user should use the admin user unique Telnet login *user*@**admin** (and also be a member of groups **root-system** and **cisco-support**).
- The devices must have one of the following SNMP community privileges: **SDROwner**, **SystemOwner**, or the default (which means no specific level was specified). You may configure this as needed, using the following guidelines.

  snmp-server community [**clear | encrypted**] *community-string* [**view** *view-name*] [**RO | RW**] [**SDROwner | SystemOwner**] [*access-list-name*]

  The **snmp-server** command takes the following arguments.

Argument	Description
[**clear	encrypted**] *community-string*	Specifies the *community-string* command format and how it should be displayed in the **show running** command output. • **clear**—*community-string* is clear text and should be encrypted when displayed by **show running**. • **encrypted**—*community-string* is encrypted text and should be encrypted when displayed by **show running**.
[**view** *view-name*]	Specifies the previously-defined view *view-name*, which defines the objects available to the community.

Argument	Description
[**SDROwner**|**SystemOwner**]	Controls what Prime Network users can see in Prime Network Vision. • **SDROwner**—Limits access to the Service Domain Router (SDR) owner. In other words, the Prime Network user will be able to view SDR owner modules and ports and SDR child modules. But the Prime Network user will *not* be able to see the contents under SDR child modules and utility cards, such as fans, power supplies, and so forth. **Note** For CRS devices running Cisco IOS XR 3.5.*x* and earlier, use **LROwner** instead of **SDROwner**. • **SystemOwner**—Does not limit access; Prime Network users will be able to see the entire physical inventory (including utility cards) in the GUI clients. Use this for CRS devices.
[*access-list-name*]	The list that contains IP addresses that are allowed to use *community-string* to access the SNMP agent.

Cisco StarOS Devices—Required Settings

The following shows how to set the StarOS settings:

```
[local]asr5000# configure
[local]asr5000(config)# snmp community name community-string read-only
[local]asr5000(config)# end
```

To verify the SNMP settings:

```
[local]asr5000# show snmp communities
Community Name                  Access Level
--------------                  ------------
private                         read-write
public                          read-only
[local]asr5000#
```

The following are required for StarOS devices:

```
snmp community name community-string read-only
snmp target target-name target-IP security-name community-string version 2c traps
snmp trap enable all target target-name
```

These are required to enable traps for IPSec tunnels on the ASR 1000:

```
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server source-interface traps gigabitEthernet 0
```

Starting from StarOS 14.0, following MIBs have been disabled by default in the device.

- ENTITY-MIB
- F-MIB
- ENTITY-STATE-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB

Note Enable the CISCO-ENTITY-FRU-CONTROL-MIB only for Physical devices and not for virtual devices.

Physical inventory will not get modeled if these mibs are disabled. Enable the MIBs using the following:

```
configure
snmp mib ENTITY-MIB
snmp mib IF-MIB
snmp mib ENTITY-STATE-MIB
snmp mib CISCO-ENTITY-FRU-CONTROL-MIB (enable the snmp mib CISCO-ENTITY-FRU-CONTROL-MIB
only for physical devices and not for virtual devices)
```

To verify if above MIBs are enabled:

```
show snmp server
```

To disable domain lookups (which can cause Telnet command delays):

```
configure
configure context context-name
no ip domain-lookup
```

Reduced Polling

Reduced polling is supported on all StarOS devices, but the fail-safe mechanism is not supported. This is because the mechanism polls the device's complete command history (from the archive log) to ensure that no device configuration changes were missed, but StarOS devices do not support the archive log.

Setting the configuration-monitor is required for reduced polling.

```
[local]asr5000# configure
[local]asr5000(config)# cli configuration-monitor
[local]asr5000(config)# end
```

To verify that the configuration-monitor is enabled:

```
[local]asr5000# show cli configuration-monitor
config monitor enabled?     :  yes
monitoring config changes?  :  yes
monitoring enabled/disabled :  Wed May 23 01:41:37 2013 cli config monitor instance :  0
cli config monitor status   :  running - idle
# config change traps sent  :  0
seconds until next monitor  :  713
longest checksum time (sec) :  0
time of last object change  :  (not set) last config object changed  :  (no changes)
```

If a device is generating configuration change events but Prime Network is not recognizing them, edit the VNE properties (Events tab) and add the IP address you want the VNE to listen to. See VNE Properties: Events, page D-17.

Cisco Nexus OS Devices—Required Settings

General Requirements

The complete hostname, such as *hostname*#, must be added when entering the credentials.

Nexus Devices with Virtual Context Devices (VDCs)

For Nexus devices with VDCs (for example, the Nexus 7000), each VDC must be configured using the procedures below so that Prime Network can process device events and monitor the devices using the reduced polling mechanism.

Note If a Nexus device contains a VDC and the VDC is not properly configured, the VNE will remain in the Unsychronized investigation state.

1. In the default VDC for the Nexus device, the **vdc combined-hostname** command must be configured.
2. To configure the VDC, enter the following commands. These commands create the VDC and enter configuration mode, display the interface membership for the VDC, allocate one interface to the VDC (ethernet 2/1 in this example), exit configuration mode, display VDC status information, and update the startup configuration file.

```
switch# config t
switch(config)# vdc vdcname
switch(config-vdc)# show vdc membership
switch(config-vdc)# allocate interface ethernet 2/1
switch(config-vdc)# exit
switch(config)# show
switch(config)# copy running-config startup-config
```

3. Associate the management IP address of all VDCs with the default VDC's *management-VRF* (that is, the VRF which is associated with the management IP address of the Nexus switch).
   a. Configure each VDC with a management IP address:

```
interface mgmt0
ip address ip-address/mask
```

   All events generated from the VDC will use the source IP *ip-address*.

   b. Add each VDC's management IP address to the Event-Generating IP field in the VNE properties (Events tab) so that the VNE will also listen to those addresses. See VNE Properties: Events, page D-17.

   c. Enable logging:

```
switch(config) logging server gateway-IP 5 use-vrf management-VRF
```

4. Ensure the system administrator account on the device is set up.
5. Verify that the VDC configuration is complete and confirm that you can switch between VDCs by entering the **switchto vdc** command as follows (*vdcname* is the name of the VDC you created, and *vdcname2* is the name of a different VDC).

```
switch# switchto vdc vdcname
 Do you want to enforce secure password standard (yes/no) [y]: no
 Enter the password for "admin":
 Confirm the password for "admin":
             ---- Basic System Configuration Dialog VDC: 4 ----
Would you like to enter the basic configuration dialog (yes/no): no
switch-cisco3# switchback
switch# switchto vdc vdcname2
switch-cisco3#
```

Reduced Polling

Reduced polling is supported on all NexusOS devices. This device type also supports failsafe mechanism.

Cisco Carrier Packet Transport Devices—Required Settings

The following settings are required for Prime Network to properly model Cisco Carrier Packet Transport devices. Configure these settings using the Packet Transport System View GUI.

- The SNMP host settings must set in the Provisioning tab (in the SNMP area).
- The Syslogs destinations must be set in the Maintenance tab (in the Syslog area).
- In the CTC GUI, do *not* specify the community string as **cellbus**.

When creating the Prime Network CPT VNE, the VNE's Telnet prompt must be configured correctly, as shown in the following procedure.

Step 1 Check the **Enable** check box and choose **Telnet** from the Protocol drop-down list (use the default port, which is 23).

Note To verify a device's Telnet sequence, open a Telnet session to the device and copy the information. The following is an example.

Step 2 Enter the expected device prompts and responses:

a. Enter **Login:** in the Prompt field.
b. Enter your user ID in the Run field.
c. Click **Add**.
d. Enter **Password:** in the Prompt field.
e. Enter the password associated with the user ID in the Run field.
f. Click **Add**.
g. Enter **#** (a hash mark) in the Prompt field.
h. Click **Add**.

For information on how to configure CPT devices using the Packet Transport System View, refer to the Cisco Carrier Packet Transport documentation.

These settings should also be configured:

- Configure the snmp community setting on the NGXP card:

  snmp-server community *community-string* **RO**

- Disable domain lookups (which can cause Telnet command delays):

  no ip domain-lookup

Reduced Polling

Reduced polling is supported on all CPT devices. If a device is generating configuration change events but Prime Network is not recognizing them, edit the VNE properties (Events tab) and add the IP address you want the VNE to listen to. See VNE Properties: Events, page D-17.

As stated earlier, reduced polling is not supported when a device is running in CTC mode.

Cisco Unified Computing System Devices—Required Settings

Communication Management Settings

Note If you use Network Discovery to create UCS VNEs, Prime Network does the following:

- If Telnet is being used, it enables HTTP on the VNE and populates the HTTP credentials fields with the Telnet credentials.
- If SSH is being used, it enables HTTPS on the VNE and populates the HTTPS credentials fields with the SSH credentials.

On the UCS device, SNMP, Telnet, and HTTP/HTTPS must be configured so that Prime Network can access the device. The recommended method for configuring this is for a user with Administrator privileges to use the UCS Manager to confirm the proper settings. (These settings are normally found under the Admin tab by expanding **All > Communication Management > Communication Services**.)

- In the Telnet/HTTP and HTTPS sections:
  - Ensure that Enable is selected.
  - Do not change the ports (use the defaults).
- In the SNMP section, ensure that Enable is selected and:
  - The Community/Username section contains the correct community string.
  - The SNMP Trap destination section contains the Prime Network gateway IP address and port, and the SNMP version. (This assumes the Event Collector is running on the gateway, which is the default Prime Network configuration. If the Event Collector is running on a unit, enter the IP address and port of the unit.)

In Prime Network, create the UCS VNE and correctly configure the VNE's Telnet, SNMP, and HTTP settings:

1. In the Telnet/SSH tab, add the Telnet/SSH credentials of the UCS device.
2. In the SNMP tab, add the snmp community string.
3. In the HTTP tab, enable HTTP/HTTPS (use the default ports).

Syslog Settings

Syslogs must be enabled and configured on the UCS devices. These settings are normally found under the Admin tab by expanding **All > Faults, Events, and Audit Log > Syslogs**.

Reduced Polling

Reduced polling is not supported on UCS devices.

Cisco ME 1200 Devices—Required Settings

Device Configuration Settings

Note If you use Network Discovery to create ME 1200 device, Prime Network does the following:

- If Telnet is being used, it enables HTTP on the VNE and populates the HTTP credentials fields with the Telnet credentials.
- If SSH is being used, it enables HTTPS on the VNE and populates the HTTPS credentials fields with the SSH credentials.

On the ME 1200 device, SNMP, and HTTP or HTTPS must be configured so that Prime Network can access the device. The recommended method for configuring this is for a user with Administrator privileges to use the ME 1200 device to confirm the proper settings.

- In the HTTPS or HTTPS sections:
  - Ensure that Enable is selected.
  - Do not change the ports (use the defaults).
- In the SNMP section, ensure that Enable is selected and:
  - The Community or Username section contains the correct community string.
  - The SNMP Trap destination section contains the Prime Network gateway IP address and port, and the SNMP version. (This assumes the Event Collector is running on the gateway, which is the default Prime Network configuration. If the Event Collector is running on a unit, enter the IP address and port of the unit.)

In Prime Network, create the ME 1200 device and correctly configure the VNE's SNMP, and HTTP settings:

1. In the SNMP tab, add the snmp community string.
2. In the HTTP tab, enable HTTP or HTTPS (use the default ports).

All Cisco Devices Added Using SSH—Required, Recommended, and Rollback Device Settings

This SSH information applies to all device types and operating systems. You will need the SSH username and password for the device. (For information on how to set up a device to run SSH, see your device documentation.) The following is an example of how to enable SSH on Cisco devices when they need to be added to Prime Network using SSH:

```
(config) ip domain-name DOMAIN
(config) crypto key generate rsa
```

Note When you are requested to enter the modulus length, leave the default value. Although a longer modulus length may be more secure, it takes longer to be generated and used.

Configure vty to accept local password checking:

```
line vty 0 4
login local
```

The following are *recommended* SSH configuration settings:

```
ip ssh time-out 120
ip ssh authentication-retries 2
ip ssh version 1(2)
```

To roll back to the original device configuration, use the following settings:

```
no ip ssh {timeout | authentication-retries}
crypto key zeroize rsa
```

SNMP Traps and Informs—Required Device Settings

The required settings for SNMP traps and informs are listed below. Note the additional information for Cisco IOS XR devices.

- Required Settings for All SNMP Traps, page A-12
- Required Settings for SNMPv1 and SNMPv2 Traps, page A-13
- Required SNMP Settings for SNMPv3 Traps, page A-13
- Required Settings for SNMP Informs, page A-14
- Recommended and Optional SNMP Settings for Cisco IOS XR Devices, page A-15

Required Settings for All SNMP Traps

```
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps chassis
snmp-server enable traps module
snmp-server enable traps bgp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ipmulticast
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps rtr
snmp-server enable traps mpls ldp
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server trap-source interface_name
```

Note *interface_name* is the active management IP address. This setting is required if the device has a management IP address.

Required for Nexus devices:

```
snmp-server enable traps
snmp-server host event_collector_IP use-vrf management-VRF
```

Note *management-VRF* is the VRF which is associated with the management IP address of the Nexus switch.

Required for ASA devices:

```
snmp-server host management-IP gateway-IP community version version
```

To enable all traps:

Caution Enabling all traps could result in a trap flood. To configure a filter that will drop certain traps or syslogs (such as ciscoConfigManEvent traps), see Filtering Out ”Pure Noise“ Traps Using the ciscoConfigManEvent Trap Filter, page 8-27.

```
snmp-server enable traps config
snmp-server enable traps syslog
```

Required Settings for SNMPv1 and SNMPv2 Traps

For SNMPv1 traps:

```
snmp-server host event_collector_IP version 1 community
```

For SNMPv2 traps:

```
snmp-server host event_collector_IP {traps | informs} version 2c community
```

Required SNMP Settings for SNMPv3 Traps

SNMPv3 With Authentication

Note *MyUsr*, *MyGrp*, *MyPswd*, and *MyView* must match the information you enter when you create the VNEs in Prime Network.

- For all devices:

```
snmp-server group MyGrp v3 priv write MyView
snmp-server view MyView internet included
snmp-server view MyView 1.2.840.10006.300 included
snmp-server group MyGrp v3 auth [notify MyView]
```

- For Cisco IOS, Cisco IOS XE, and CatOS devices:

```
snmp-server user MyUsr MyGrp v3 auth {md5|sha} MyPswd
```

- For Cisco IOS XR devices:

```
snmp-server user MyUsr MyGrp v3 auth {md5|sha} {WORD,CLEAR,encrypted} MyPswd
SystemOwner
```

- For all devices, after configuring SNMPv3 on the device, configure the following setting:

```
snmp-server host event_collector_IP traps version 3 auth MyUsr
```

SNMPv3 With Privacy and Authentication

Note *MyUsr*, *MyGrp*, *MyAuthPswd, MyPrivPswd*, and *MyView* must match the information you enter when you create the VNEs in Prime Network.

- For all devices:

```
snmp-server group MyGrp v3 priv write MyView
snmp-server view MyView internet included
snmp-server view MyView 1.2.840.10006.300 included
snmp-server group MyGrp v3 priv [notify MyView]
```

- For Cisco IOS, Cisco IOS XE, and CatOS devices:

```
snmp-server user MyUsr MyGrp v3 auth {md5|sha} MyAuthPswd priv {des|aes 128|aes
192|aes 256} MyPrivPswd
```

- For Cisco IOS XR devices:

```
snmp-server user MyUsr MyGrp v3 auth {md5|sha} {WORD,CLEAR,encrypted} MyAuthPswd priv
{des|aes 128|aes 192|aes 256} {WORD,CLEAR,encrypted} MyPrivPswd  SystemOwner
```

- For all devices, after configuring SNMPv3 on the device, configure the following setting:

```
snmp-server host event_collector_IP traps version 3 priv MyUsr
```

SNMPv3 No Authentication

Note *MyNoAuthUsr* and *MyNoAuthGrp* must match the information you enter when you create the VNEs in Prime Network.

- For Cisco IOS, Cisco IOS XE, and CatOS devices:

```
snmp-server group MyNoAuthGrp v3 noauth
snmp-server user MyNoAuthUsr MyNoAuthGrp v3
```

- For Cisco IOS XR devices:

```
snmp-server user MyNoAuthUsr MyNoAuthGrp v3 SystemOwner
```

- For all devices, after configuring SNMPv3 on the device, configure the following setting:

```
snmp-server host event_collector_IP traps version 3 noauth MyNoAuthUsr
```

Required Settings for SNMP Informs

SNMP Informs can be configured for all SNMPv3 modes. The following is an example for configuring SNMPv3 Informs for the mode SNMPv3 With Privacy and Authentication. The configuration is similar for the other modes (refer to the required settings for each mode for guidelines).

Note For Informs, *MyUsr* corresponds to Prime Network's local user (not the device-configured user that is used for polling and receiving traps).

- For Cisco IOS, Cisco IOS XE, and CatOS devices:

```
snmp-server user MyUsr MyGrp remote event_collector_IP v3 auth {md5|sha} MyAuthPswd
priv {des|aes 128|aes 192|aes 256} MyPrivPswd
```

- For Cisco IOS XR devices:

```
snmp-server user MyUsr MyGrp remote event_collector_IP v3 auth {md5|sha}
{WORD,CLEAR,encrypted} MyAuthPswd priv {des|aes 128|aes 192|aes 256}
{WORD,CLEAR,encrypted} MyPrivPswd  SystemOwner
```

- For all devices, after configuring SNMPv3 on the device, configure the following setting:

```
snmp-server host event_collector_IP informs version 3 priv MyUser
```

Recommended and Optional SNMP Settings for Cisco IOS XR Devices

In large-scale environments that contain more than 100 EFPs or PWs associated with the same interface/subinterface, an interface outage may generate a large number syslogs and traps. In such scenarios we recommended that you increase the default snmp server queue length buffer size using the following command. This applies to Cisco IOS XR 4.0 and later. The value of *new-buffer-size* should at least equal the number of EFP or PW objects. (This increase is also advisable if traps are being used as a transport mechanism for syslogs by way of the CISCO-SYSLOG-MIB.)

```
snmp-server queue-length new-buffer-size
```

If a Cisco IOS XR device has a configured virtual IP address *and* the VNE was added using that address, the device can receive the traps and syslogs through the virtual IP address. You do not need to configure the source for the SNMP traps and syslogs in the Prime Network Administration GUI client, as described in VNE Properties: Events, page D-17. The following are examples of commands for configuring a virtual IP address:

```
ipv4 virtual address 10.49.224.120 255.255.255.128
ipv4 virtual address use-as-src-addr
```

To enable all traps to be sent from a Cisco IOS XR device:

```
snmp-server traps <CR>
```

Alternatively, choose from the following list to enable forwarding of specific traps from Cisco IOS XR devices:

```
snmp-server trap link ietf
snmp-server traps rf
snmp-server traps bfd
snmp-server traps ethernet cfm
snmp-server traps ds1
snmp-server traps ds3
snmp-server traps ntp
snmp-server traps ethernet oam events
snmp-server traps otn
snmp-server traps copy-complete
snmp-server traps snmp linkup
snmp-server traps snmp linkdown
snmp-server traps snmp coldstart
snmp-server traps snmp warmstart
snmp-server traps snmp authentication
snmp-server traps flash removal
snmp-server traps flash insertion
snmp-server traps sonet
snmp-server traps config
```

```
snmp-server traps entity
snmp-server traps syslog
snmp-server traps system
snmp-server traps ospf lsa lsa-maxage
snmp-server traps ospf lsa lsa-originate
snmp-server traps ospf errors bad-packet
snmp-server traps ospf errors authentication-failure
snmp-server traps ospf errors config-error
snmp-server traps ospf errors virt-bad-packet
snmp-server traps ospf errors virt-authentication-failure
snmp-server traps ospf errors virt-config-error
snmp-server traps ospf retransmit packets
snmp-server traps ospf retransmit virt-packets
snmp-server traps ospf state-change if-state-change
snmp-server traps ospf state-change neighbor-state-change
snmp-server traps ospf state-change virtif-state-change
snmp-server traps ospf state-change virtneighbor-state-change
snmp-server traps bridgemib
snmp-server traps isis all
snmp-server traps bgp
snmp-server traps frame-relay pvc interval 30
snmp-server traps atm pvc interval 30
snmp-server traps ima
snmp-server traps hsrp
snmp-server traps vrrp events
snmp-server traps vpls all
snmp-server traps vpls status
snmp-server traps vpls full-clear
snmp-server traps vpls full-raise
snmp-server traps l2vpn all
snmp-server traps l2vpn vc-up
snmp-server traps l2vpn vc-down
snmp-server traps mpls traffic-eng up
snmp-server traps mpls traffic-eng down
snmp-server traps mpls traffic-eng reroute
snmp-server traps mpls traffic-eng reoptimize
snmp-server traps mpls frr all
snmp-server traps mpls frr protected
snmp-server traps mpls frr unprotected
snmp-server traps mpls ldp up
snmp-server traps mpls ldp down
snmp-server traps mpls ldp threshold
snmp-server traps mpls traffic-eng p2mp up
snmp-server traps mpls traffic-eng p2mp down
snmp-server traps rsvp all
snmp-server traps rsvp new-flow
snmp-server traps rsvp lost-flow
snmp-server enable traps mpls l3vpn all
snmp-server enable traps mpls l3vpn vrf-up
snmp-server enable traps mpls l3vpn vrf-down
snmp-server enable traps mpls l3vpn max-threshold-cleared
snmp-server enable traps mpls l3vpn max-threshold-exceeded
snmp-server enable traps mpls l3vpn mid-threshold-exceeded
snmp-server enable traps mpls l3vpn max-threshold-reissue-notif-time 1
snmp-server traps fabric plane
snmp-server traps fabric bundle link
snmp-server traps fabric bundle state
snmp-server traps sensor
snmp-server traps fru-ctrl
```

Syslogs—Required Device Settings

The following table lists the settings you must configure for syslogs.

Note If you are using reduced polling, be sure to follow the requirements in this section. These settings increase the depth of syslogs that will be logged, and ensures that all syslogs are handled. If the device is using Cisco IOS XR, verify the syntax of the settings against the Cisco IOS XR documentation in case there have been changes across OS releases.

If a device is generating configuration change events but Prime Network is not recognizing them, edit the VNE properties (Events tab) and add the IP address you want the VNE to listen to. See VNE Properties: Events, page D-17.

Required Settings	

All	`logging gateway_IP`
	
	Required if the device has a management IP address (*interface_name* is the active management IP address):
	`logging source-interface interface_name`

Cisco CatOS,
Cisco IOS,
and Cisco IOS XE
	`logging on`
	`logging buffered 64000 informational`
	`logging trap informational`
	`logging event link-status default`
	
	Required for ASR 1000 IPSec Syslogs:
	`crypto logging session`
	
	Required for MPLS TP-related changes:
	`mpls tp`
	`[no] logging events`
	`[no] logging config-change`

Required Settings	

Cisco IOS XR	`logging on`
	`logging events level informational`
	`logging buffered <307200-125000000>`
	
	Note The range indicates the minimum of 307200 and maximum of 125000000 log messages that can be stored on the device
	
	`logging trap informational`
	`logging events link-status software-interfaces`
	
	If you will be using Path Tracer or event correlation to mimic flows that involve bridge tables, configure the following:
	`l2vpn resynchronize forwarding mac-address-table location node-id`
	
	Note If devices are running an older version of Cisco IOS XR, enable the following commands to make sure Prime Network is properly notified of link status changes:
	`logging events link-status logical`
	`logging events link-status physical`

Cisco Nexus OS	If you are using reduced polling, specify the following for each VDC that is configured in the Nexus device. `logging server` *`gateway-IP`* `5 use-vrf` *`management-VRF`* If you are *not* using reduced polling, specify one of the following (for each VDC): `logging server` *`gateway-IP`* `use-vrf` *`management-VRF`* `logging server` *`gateway-IP facility`* `use-vrf` *`management-VRF`* **Note** *`management-VRF`* is the VRF which is associated with the management IP address of the Nexus device.
Cisco ASA OS	`logging host` *`management-IP gateway-IP`*

IP Address Configuration for Traps, Syslogs, and VNEs

Traps and syslogs maybe dropped if any of the VNEs managed by Prime Network are configured in such a way that the following addresses are *different*:

- The traps and syslogs source IP address
- The VNE IP address (entered when the VNE was created and displayed in the VNE properties)

To avoid missing any traps or syslogs, do one of the following:

- Change the device configuration so that traps and syslogs are sent using the VNE's IP address. In addition, make sure that the source IP address matches the startup-config.
- Configure the VNE to receive traps and syslogs using a different IP address by changing the VNE Properties: Events, page D-17. Do this if a device is generating configuration change events but Prime Network is not recognizing them.

Note If your deployment has virtual entities that generate events, such as applications running on virtual machines, add the entity's IP address in the VNE Events tab. Refer to VNE Properties: Events, page D-17 for more details.

TACACS, TACACS+, RADIUS Integration - Required Device Settings

The following table lists the settings that must be configured at a minimum for a device using TACACS, TACACS+, and RADIUS. The user must also have sufficient permissions to run these commands.

Required Settings	
Cisco CatOS, Cisco IOS, Cisco IOS XE, IOS XR, CPT, Nexus OS	`terminal length` *`lines`* `terminal width` *`characters`* `terminal default exec prompt timestamp` where, *lines* = Must be integer ranging from 5 to 512. Setting length to 0 allows an infinite number of rows to be displayed on a screen. *characters* = Number of characters to display on a screen. Must be followed by integer ranging from 5 to 512
StarOS	`terminal length` *`lines`* `terminal width` *`characters`* where, *lines* = Must be integer ranging from 5 to 512. Setting length to 0 allows an infinite number of rows to be displayed on a screen. *characters* = Number of characters to display on a screen. Must be followed by integer ranging from 5 to 512