Configuring Device Credentials for Y.1371 SLA and Ethernet Flow Point Reports

The following topics show you how configure the Telnet and SSH access credentials which are required if you plan to enable ITU-T Y.1371 SLA and Ethernet flow point QoS reports on devices running IOS-XR:

Adding Telnet and SSH Credentials

Y.1731 reports can be enabled on devices running IOS and IOS-XR, and Ethernet flow point QoS reports can be enabled on devices running IOS-XR. Before you enable these reports, you must add the device Telnet or SSH credentials to Prime Performance Manager. To add the Telnet or SSH credentials:

Step 1 Log into the Prime Performance Manager GUI as the administrative (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 Click the **Telnet/SSH** tab.

Step 4 In the Device Credentials Editor toolbar, click the **Add a New Device Credential for a Device** tool.

Step 5 In the Add a Credential dialog box, enter the following:

- User Name—Enter the device login user name.
- Password—Enter the password for the login user.
- Enable User Name—Enter the privileged user name.
- Enable Password—Enter the privileged user password.
- Protocol—Choose the transport protocol to be used to communicate with device:
  - Telnet—Telnet
  - SSHv1—SSH Version 1
  - SSHv2—SSH Version 2
  - WSMA_SSH—Web Services Management Agent over SSHv2. WSMA is an infrastructure framework that allows external applications to monitor and control Cisco devices. WSMA uses transports such as SSH, HTTP, and HTTPS to access a set of Web Services agents residing on the Cisco device.

- Port—The device port to be used by the transport protocol chosen in the Protocol field.

- Sub System—The subsystem used by transport protocol. If the subsystem is defined on the device, enter it here. A blank string is the default subsystem for SSH. The default subsystem for WSMA is "wsma".

Step 6 Click **OK**.

The new credential is added to the Telnet/SSH credential table.

Step 7 Test the credential:

a. In the new credential table row Actions column, click the **Test the Credential** tool.

A Testing Credentials for [*device name*] window appears. If Prime Performance Manager succeeded in connecting to the device with the credentials you entered, the following is displayed:

```
****Starting Credentials Test****
Connection test successfully!
****Test Completed****
```

If Prime Performance Manager could not connect to the device, an error is displayed, for example:

```
****Starting Credentials Test****
Exception while connecting to device!
****Test Completed****
```

Step 8 In the Testing Credentials window, click **Close**.

Step 9 If the credentials test succeeded, on the Device Credentials Editor toolbar, click the **Save All Credentials** tool to save the new credential.

If the credentials test failed, verify the credentials with your network administrator and check network connectivity. You can update the credential and run the test again until it succeeds. Additionally, you can:

- From the Actions column, click the **Clear the Row** tool to clear the row contents or click the **Delete this Credential** tool to delete the entire credential.

- From the Device Credentials Editor toolbar, click the **Reload Credentials from the Server** tool to reload all the Telnet and SSH credentials.

After you add the Telnet and SSH credentials, you might want to perform the following tasks:

- Run device discovery. See Chapter 4, "Discovering Network Devices,"for procedures.

- Enable the Y.1731 and Ethernet Flow Point reports: click **Reports** in the navigation tree, click the **Report Status** tab, enable the **IP SLA: Y.1731** and **IP QoS: Transport and Availability** reports. For more information, see Chapter 7, "Working With Reports and Dashboards."

Telnet and SSH Credential Notes

After adding the Telnet and SSH credentials, running device discovery, and enabling the Y.1731 and Ethernet Flow Point reports, review the following information:

- Default Credential—Prime Performance Manager includes a default *.*.*.* Telnet credential. The default values are from XMP_PAL.properties file. You can edit XMP_PAL.properties to set new initial default credential. If you change the default credentials in the web GUI and save it, your new default credentials will be saved to credential file instead of property file, which means now the default credentials are from credential file.

- Device Discovery—During device discovery, the Telnet and SSH credentials of discovered devices are displayed in a table beneath the SNMP credentials. The Telnet and SSH search algorithm seeks an exact match first. If no exact match is found, the default entry is used for device Telnet/SSH access credential.

- Events—If a Telnet or SSH credential issue arises, a Credential Problem state event is displayed in the device summary indicating an issue accessing the device by its Telnet or SSH credential exists.

- Reports—Only the Y.1731 SLA and Ethernet Flow Point reports require Telnet or SSH credentials. All other reports use SNMP polling.

- Prime Network Integration—When you import device credentials from Prime Network, the protocol credential, including Telnet, SSH_v1 and SSH_v2, are imported with the SNMP credentials. For protocols not supported by Prime Performance Manager, the default protocol, Telnet, is used and relevant information is logged.

Tip   To view detailed information about a device inventory import, click the question mark icon in Prime Performance Manager toolbar.

- Commands—Telnet and SSH credentials can be managed using the following commands:

  - ppm addcreds—Adds the Telnet and SSH credentials to access the device. See ppm addcreds, page B-5.

  - ppm showcreds—Shows the Telnet or SSH credential configured for a device. See ppm showcreds, page B-44.

  - ppm deletecreds—Deletes the Telnet or SSH credential from the device. See ppm deletecreds, page B-16.

  - ppm xmlpoll—Retrieves the device XML output. See ppm xmlpoll, page B-63.