# Cisco Prime Provisioning 6.4.1 Release Notes

**July 29, 2013**
**OL-27133-02**

Cisco Prime Provisioning 6.4.1 maintenance release introduces a new mechanism for customizing policies, that combines and simplifies the process of adding new attributes, and creating CLI templates related to a policy, as well as enhancements for EVC Pseudowire services and MPLS VPN services in Cisco Prime Provisioning. It is the first maintenance release based on Prime Provisioning 6.4.

You can install Cisco Prime Provisioning 6.4.1 on Cisco Prime Provisioning 6.4 or 6.4.0.1 or 6.4.0.2 based server. Schema upgrade is supported from 6.2.1.50/ 6.3.0.3/ 6.4 / 6.4.0.1 / 6.4.0.2 to 6.4.1.

See the New Features and Enhancements in Prime Provisioning 6.4.1, page 3 for a list of point patches whose enhancements and defect resolutions have been merged into 6.4.1.

All documentation, including this *Cisco Prime Provisioning 6.4.1 Release Notes* document and any or all parts of the Prime Provisioning 6.4 documentation set, *might* be upgraded over time. Therefore, we recommend that you access the Prime Provisioning documentation at:

http://www.cisco.com/go/provisioning

You can also navigate to this documentation set by clicking **Help** on the Home Page of the Prime Provisioning 6.4.1 product. The Related Documentation, page 23 gives the URL for the most current version of each guide to be used with Cisco Prime Provisioning 6.4.1.

The information in this *Cisco Prime Provisioning 6.4.1 Release Notes* document gives you an overview of this release and helps you understand what has changed since Cisco Prime Provisioning 6.4. Please read this document prior to reading any other guides or documents for Cisco Prime Provisioning 6.4.1.

# Contents

This document includes the following sections:



**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Installing Prime Provisioning 6.4.1

Prime Provisioning patches are available at:

http://software.cisco.com/download/type.html?mdfid=284586808&flowid=37682

For information about the installation process, see the Installation Notes section.

# Introduction

Cisco Prime Provisioning is a management solution for network fulfillment and diagnostics that enables the automation and scaling of complex, policy-driven network provisioning tasks to produce consistent and reliable service deployments. Prime Provisioning does this by planning, provisioning, and auditing services across core, aggregation, access, and consumer premises equipment devices.

Cisco Prime Provisioning enables fast deployment and time-to-market of Multiprotocol Label Switching (MPLS) and Carrier Ethernet technologies. In addition, the Prime Provisioning Traffic Engineering Management (TEM) module is Cisco's exclusive planning and provisioning tool for Cisco MPLS Traffic Engineering-enabled routers. MPLS Transport Profile (TP) provides service providers with a reliable packet-based technology that is based upon circuit-based transport networking, and hence is expected to align with current organizational processes and large-scale work procedures similar to other packet transport technologies.

The Cisco Prime Provisioning solution has management capabilities for MPLS VPN, L2VPN and Carrier Ethernet, MPLS Diagnostics, MPLS TP, and MPLS Traffic Engineering. These capabilities that comprise Cisco Prime Provisioning can be used in a stand-alone manner or can be integrated with IP-NGN Suite.

Cisco Prime Provisioning 6.4.1 has new functionality added and changed since Prime Provisioning 6.4 (see the "New Features and Enhancements in Prime Provisioning 6.4.1" section on page 3) and fixes to problems (see the "Prime Provisioning 6.4.1 Resolved Bugs" section on page 20).

The system recommendations for Prime Provisioning 6.4.1 (see the "System Recommendations" section on page 3) are based on those for Prime Provisioning 6.4 (with some restrictions, as noted). The new devices and platforms supported in addition to those supported in Prime Provisioning 6.4 are referenced in the "System Recommendations" section on page 3.

Steps for installing Prime Provisioning 6.4.1 are found in the "Installation Notes" section on page 14, and other important information is found in the "Finding Known Problems in Prime Provisioning 6.4.1" section on page 23. For problems that were found and might still exist in Prime Provisioning 6.4.1, see the URL in the Prime Provisioning 6.4.1 Resolved Bugs, page 20.

URLs for base information about Prime Provisioning 6.4.1 and an overview and suggested reading order of these documents is given in the *Cisco Prime Provisioning 6.4 Documentation Overview*.

The Prime Provisioning 6.4.1 documentation includes the Prime Provisioning 6.4 document set and the updated information for Prime Provisioning 6.4.1 found in this *Cisco Prime Provisioning 6.4.1 Release Notes.* The entire documentation set is listed in the "Related Documentation" section on page 23.

# System Recommendations

The system recommendations and requirements are listed in Chapter 1, System Recommendations, of the *Cisco Prime Provisioning 6.4 Installation Guide*. For details on network devices and related software supported with Prime Provisioning 6.4.1, refer to *Cisco Prime Provisioning Supported Devices*.

We recommend that you thoroughly review that list before even planning your installation, to be sure you have all the hardware and software needed for a successful installation. We also recommend that you review the section Important Notes, in this release note in order to be aware of any known system, installation or other issues in the current release.

# New Features and Enhancements in Prime Provisioning 6.4.1

This section describes features and enhancements added or modified in Prime Provisioning 6.4.1.

For system recommendations, refer to the Cisco Prime Provisioning 6.4 Installation Guide, and for device and platform support, refer to Cisco Prime Provisioning Supported Devices. It includes the network devices and related software supported with Prime Provisioning 6.4.1. We recommend that you thoroughly review this list before even planning your installation, to be sure you have all the hardware and software needed for a successful installation. We also recommend that you review the section Installing Prime Provisioning 6.4.1, page 2, in this release note in order to be aware of changes to the installation or upgrade procedure.

Prime Provisioning 6.4.1 is based on Cisco Prime Provisioning 6.4.

Prime Provisioning 6.4.1 includes problems fixed since Cisco Prime Provisioning 6.4. See Prime Provisioning 6.4.1 Resolved Bugs, page 20.

**Note** With this release, Prime Provisioning can be used as a standalone product or as part of the Cisco Prime for IP Next Generation Network (IP NGN) Suite. When installed as part of the suite, you can launch Prime Provisioning from the Prime Central portal. For more information about Prime Central, see the documentation for Cisco Prime Central.

Items specific to Prime Provisioning 6.4.1 include the new and changed information as documented in the following sections:

- Customizing EVC and MPLS Policies, page 4
- Pseudowire Headend Interface, page 9
- L2VPN/EVC/TDM-CEM/ATM New Features, page 10
- MPLS VPN New Features, page 13

# Customizing EVC and MPLS Policies

In Prime Provisioning you can now embed customized command line interface (CLI) templates into EVC and MPLS policies. You can also extend policies by adding attributes that you define directly in the policy screen.

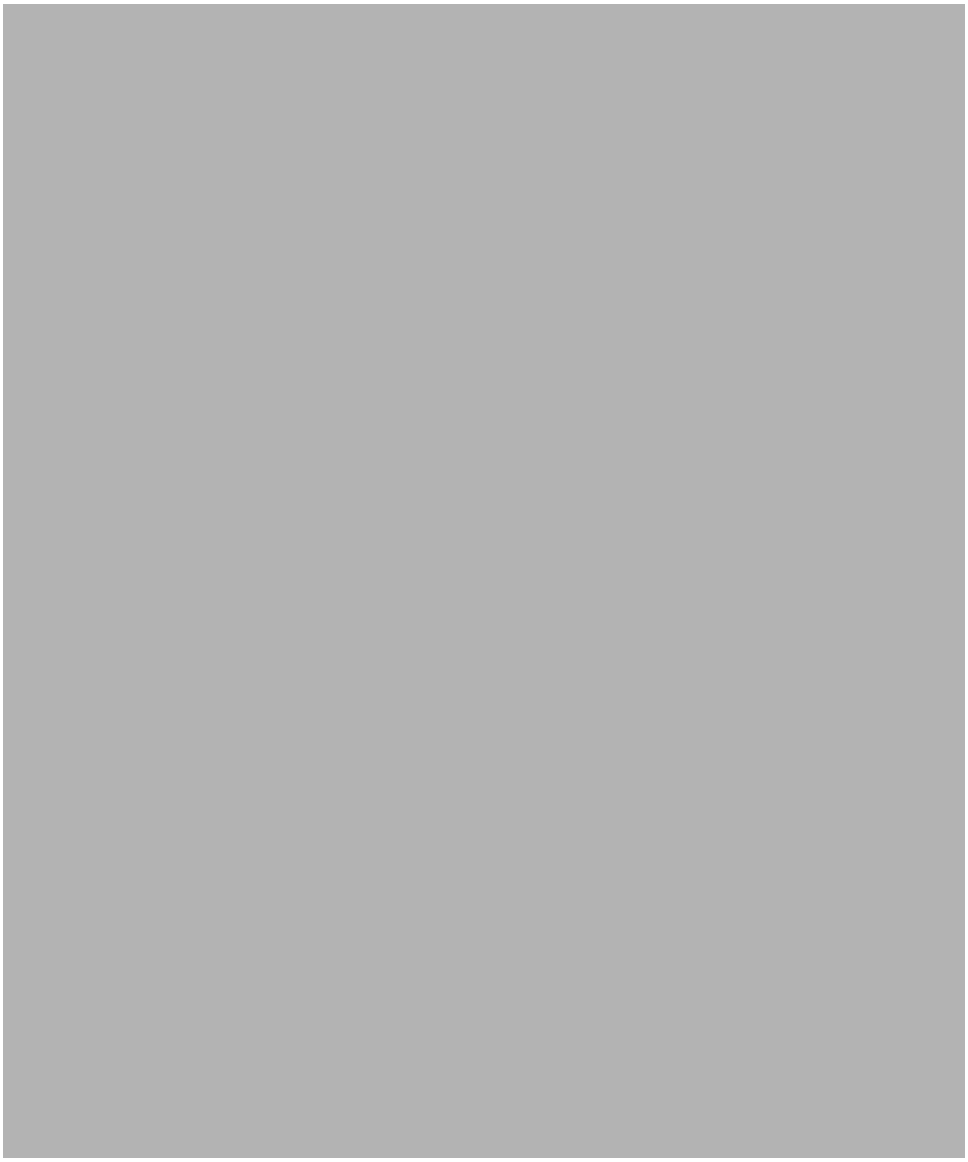
This new feature simplifies the process of executing the following Prime Provisioning tasks:

- Additional Attributes- which required you to define new UI attributes in a separate XML file. The new attributes defined in the policy behave in a manner similar to the existing feature, but allow you to define the templates inline.
- Template and Data File Manager- The new CLI templates in the policy are simpler to use, and allow you to create and use CLI customizations without the need for data files. However, when you upgrade using an existing database, it is not possible to convert existing templates into the new form of CLI templates automatically.

## Adding New Attributes to a Policy

While creating EVC and MPLS policies, a new **Create UI Group** button on every page of the policy enables you to create any number of UI groups on any number of pages on the policy. For example, as shown in the figure below, you can create a new UI group called **Security aspects** using the **Create UI Group** button.

*Figure 1 An EVC Policy with Four UI Groups.*



The name (in this example, **Security aspects**) you provide for the UI Group appears as the title of the new section. Once you create a UI group, the **Create** button and the Settings icon is displayed in the title bar, enabling you to create attributes. You can further edit, delete and reorder attributes within the UI group. You can add attributes only to UI groups you create, and not to existing groups in the policy. Using the **Create** button, you can specify the type of attributes that you want to create. The types that you can specify are:

- String – regular expression and length bounds for validation
- Password – similar to the string attribute but masked in UI
- Integer – requires you to enter numbers and defines a range
- Hexadecimal – requires you to enter hexadecimal values
- Enumeration - drop-down list

- Check box – provides a check box
- IPv4 – IP v4 address, may define range
- IPv6 - IP v6 address, may define range
- Device – pick devices from the inventory – filter by device role
- Device Interface – pick device interfaces from the inventory

Using the name given to every attribute, you can refer to the value of that attribute from a CLI template. For example, if you create an attribute called *cbr*, using a CLI template, you can refer to this new attribute using the variable *$cbr*. Every attribute also has a display name and a description. While the display name is used as the label for the attribute in the Prime Provisioning UI, the description is displayed when you hover over the tool tip icon for that attribute.

Attributes can be marked Required or Optional. To verify whether optional values are provided, you can use *#if ( $my_optional_attribute )* within a CLI template. Attributes marked Required are displayed on the policy and Service Request pages.

A new **Create Global UI** button allows you to specify global attributes which are identical across all links of a service request. These global attributes appear on the first page of the service request. Like other attributes, global attributes can also be set as editable or non-editable, and have default values assigned to them.

### Creating Templates

You can now create and customize templates that consist of the CLIs that you want to deploy on devices. Templates can reference the data that you enter in UI groups. When you create a template, in a policy, you can specify:

- CLI Merging Mode:
  - External- This mode acts in a manner similar to the Template Manager customizations. It is suitable for adding configuration that you want Prime Provisioning to generate without modifying any lines in the configuration. Extra configuration is simply sent to the device as is.
  - Combine- This mode acts in a manner similar to the XDE/PAL customizations. It is suitable for changing the configuration that Prime Provisioning generates. The content in the template is merged with the exiting configuration, and is also sent to the device only when the current device configuration does not contain the required configuration. In addition to this, the output of the template is audited so that Prime Provisioning can verify the final device configuration and check that the configuration specified in the template is present on the device. Combining depends on the ability of Prime Provisioning's config parser (NOM) to parse the configuration generated by the template. To determine whether this Combine mode can be used with a given template, you need to merely preview the configuration generated for a service request. If NOM does not recognize a line from the template, you will see an error and the line is not included in the final configuration.
  - ExternalWithModify - To modify the customized template attribute value, this CLI merging mode has to be selected.
- Commission Sequence: Determines whether the commission cli is added before or after the configuration that Prime Provisioning generates. To ensure that Prime Provisioning sets up the basic service before it adds the features in the template, select **After**. If the merge mode you select is **Combine** and the commission sequence you select is **After**, the template can overwrite or remove the configuration that Prime Provisioning generated. Instead, if the commission sequence you select is **Before,** it will be Prime Provisioning's configuration that can overwrite that of the template.
- Commission CLI: The CLI generated during the commission sequence specified in the Velocity Template Language.

- Decommission Sequence: Determines whether the decommission cli configuration is removed before or after the configuration that Prime Provisioning generates by default. This is the opposite of the Commission Sequence. To control the decommissioning sequence individually, you can create a separate template solely for the purpose of decommissioning.
- Decommission CLI: The CLI created during the decommission sequence.
- Verify: Click the **Verify** button after entering into CLI lists the missed out variable name, which is defined in the policy page but wrongly declared in the CLI section.

**Variable Completions for Specifying CLIs:**

Variable completions are now available while specifying CLIs in templates. This means that you can use Ctrl-Space for completion of variables that you want to enter. For example, when you type $ and then type Ctrl-Space, the list of all possible variables is displayed and you can select variables directly from this list without having to know them beforehand. Similarly if you type a prefix to a variable e.g. $SR, then a filtered list of all $SR variables is listed. Further typing while the variable list is visible will further narrow the available options. When only a single option is available, it is selected automatically.

The displayed list of variables consists of

- customized attributes that you define in the UI groups.
- $SR. standard attributes from the service request section for template attributes. These are the same attributes (names and values) as are defined for the template manager.
- the configuration of the device in the form of an XML document as parsed by NOM is present in the variable $DeviceConfig
- the definition of the service to be configured as represented in the Database is also available as an XML document in the variable $ServiceIntent. This can be used if you need to get some aspect of the service which is not available in the $SR prefixed variables.
- $system.xpath (<XML>, <XPATH query>)
- $list.xpath (<XML>, <XPATH query>)
- $system.xpathreference (<XML>, <XPATH query>)
- $list.xpathreference (<XML>, <XPATH query>)
- variables that return sections of XML documents queried using XPATH (The $list variants will return a list of matches while the $system variants return the first matched element if any. The reference variants do not create a copy of the parts of the XML document that are returned.):
- $system.log()– logs a message in the http log.
- $system.print()– prints a message in the http.out log.
- $system.throwException() exception name, message (For example, “MPLS.customization”, “MPLS service cannot be provisioned because of ..”)– This is useful to throw a validation error, No configuration will be deployed. A deployed Service Request deploy that throws an exception transitions to the Invalid state and the exception message is shown in the task log and in the configuration preview.
- $DeviceCredentials. A set of device inventory related attributes for testing properties of the device.

### Creating Rules for Templates

Every template can be associated with a set of rules that determine the type of devices on which the template can be deployed. This allows you to generate different CLIs for devices of different roles types and operating systems. Prime Provisioning deploys the template only when the criteria specified in these rules is fulfilled. When no rules are specified, the template is deployable on all devices.

You can create multiple rules for a given template. For example, you could have one rule for a template to be deployed on only IOS-XR devices of type N-PE; while another rule for the template to be deployed on IOS devices of type U-PE.

### Importing and Exporting Customizations (in XML format)

You can export customizations in an XML format and save it using a text editor to create a backup of your customization. It is recommended that you create a backup of your customizations or copy the policy and modify the copy before you modify a policy with existing service requests (see Changing Customizations when a Policy is in Use), so that you can revert back to these customizations by merely importing the same XML document that you saved. To do this, an **Import/Export** button has been provided on the policy creation page. The customizations that you export are displayed in a new browser window from which you can copy the customizaitons onto a text editor for further use.

By exporting the customization data in an XML text format, you can:

- Apply the same customization to different policies by simply exporting the XML text and importing the same over to a new policy. This is useful when you cannot copy the whole policy for example copying a customization to a policy that is already in use with service requests.
- Edit the order in which the UI groups are placed and also edit the order in which the the attributes are displayed within the UI groups.

### Changing Customizations when a Policy is in Use

The new UI attributes that you define in policies can be edited even after service requests are defined based on those policies.

To introduce a new capability for only newly created services, it is recommended that you create a new policy with this capability. This can be done by copying an existing policy to create a new one and making the current policy inactive. You can also rename the policies that you copy so that operators can use the same name for the new policy. While creating new services requests, Prime Provisioning only lists the active policies so that you do not select the inactive policies used for existing service requests. This ensures that you do not face any errors while modifying in use policies.

Changes to the attributes in the policy will cause no change to the data in the associated service requests. The changes can only be noticed in the user interface and the way the service request is configured.

To create a backup of the previous version of a customization, use the Import/Export feature explained above. This enables you to revert back to the previously saved version after modifying a policy that has existing service requests.

Some types of changes that you make to a policy can result in undesired changes to a service and hence it's recommended that you review existing service requests before you make these changes to the policy. The types of changes that requires you to review existing service requests are:

- Removing an attribute:
  When an attribute is removed from the policy page with its declaration existing still in the CLI template, an appropriate error with link "**Has errors**" is enabled in the "**Provisioning CLI Customizations**" page. On rolling over the mouse over the "Question mark" icon, the necessary details are shown. Although the removed attribute is no longer displayed and referenced from the

provisioning logic and templates, it continues to exist in the service request.The saved value reappears only if you add an attribute with the same name. This behavior is to ensure that the removal of attributes is reversible step. When you remove attributes that continue to be referenced from the provisioning logic or from templates, the templates fail because they are referring to undefined attributes. Thus it is recommended that you first remove all references to the attributes, before you proceed with the removal of these attributes.

- Removing values from the valid range of an attribute:
  This can be done by changing a string validation regular expression, restricting an integer range, and removing values for an enumeration. After you remove these values and then edit the service request, while retaining the invalid values, you will not be able to save the service request. You will need to either change the value of the attribute or cancel your edit. Thus it is recommended that you edit service requests and not use the invalid values before you change the policy.
- Making an attribute non-editable:
  The attribute can not be modified and will be hidden from the service request page create using the policy with the non-editable attribute. Attribute values modified during service request creation, are not visible to the operated modifying services. To ensure that different service requests do not have different values for the same attribute, it is recommended that all service requests created with the policy contain the same default values before they are marked non-editable. Thus new service requests can only be created with the default values.

Different changes that you make to existing service requests can have varied results. The results are:

- Adding an attribute: The next time you create or edit the service request, this attribute will be added with its default value and can be referred from the templates and provisioning logic.
- Expanding the valid range of an attribute: No changes to the existing service request, however, you can edit the service request to select the new value.
- Editing the default value for an attribute: No change to the existing service requests. Only newly created service requests will take the default value.
- Make an attribute editable: The value can be modified while creating or editing existing services. The attribute will contain its former value.

After you add new attributes to a service, which translate to more lines of configuration, and re-deploy the service, managing the transition is easy since the template will be activated automatically.

However, if you remove template configurations and replacing them with new configurations, you need to ensure that you maintain the decommissioning sequence of the old features before you add the new features. Once the service is migrated, you must no longer use the old features. To do this, you can introduce an additional attribute that represents whether the service is migrated or not. This can be used as a condition with an ‘if’ statement in the template to decide whether an old extension has to be decommissioned or not. For advanced help in migrating from template solutions to customizing policies, you can contact theh Advanced Services team.

# Pseudowire Headend Interface

Using Prime Provisioning, you can now configure an L3 VPN attachment circuit, with a Pseudowire access. Using the Pseudowire Headend feature on the ASR9000, this can be achieved without terminating the Pseudowire on an Ethernet interface, or allocating bridge domain for this purpose. This enables the creation of an end to endMPLS network where access is provided by a small switch that does not support many L3VPN instances. On that switch you configure a pseudowire which terminates on the ASR9000. There the pseudowire is directly connected to L3VPN.

To prepare to use this feature you need both an L3 VPN policy and a EVC policy.

**Step 1** Navigate to the Policy Editor page.

**Step 2** In the PE Interface details section, select the **Create virtual interface only** check box. This displays the **Configure Pseudowire Headend** check box.

**Step 3** Select the **Configure Pseudowire Headend** check box to enable the pseudowire headend feature for the PE interface.

**Step 4** Make other required changes and save the policy.
Note that the **Configure Pseudowire Headend** check box is hidden until you select the **Create virtual interface only** check box. When you use this policy to create a service request, Prime Provisioning disables the PE Interface column in the Service Request Editor. When this service is deployed, Prime Provisioning creates a pseudowire-ether interface configured in the device.

**Step 5** Create an EVC policy, this should have:

- Core type- PSUEDOWIRE
- For end to end MPLS which is the typical case, enable **CE directly connected to N-PE**.
- Ensure that the the **Configure Bridge Domain** checkbox is disabled.

Then to create services, follow these steps:

**Step 1** Navigate to **Operate > Service Request Manager**.
The Service Request Manager window appears.

**Step 2** Click **Create**.
The Service Request Editor window appears.

**Step 3** From the policy picker, choose the L3 policy that you created in steps 1-4.
The L3 VPN Service Request editor window appears. This window enables you to specify options for the service request, as well as configure links.

**Step 4** Create an EVC service request using the EVC policy created in step 5 above

**Step 5** Set the pseudowire core connectivity attributes. See table, Pseudowire Core Connectivity Attributes, for more details about the attributes.

**Step 6** Set up links to the N-PE as described in section Setting up Links to the N-PE.

**Step 7** When you have completed setting the attributes in the EVC Service Request Editor window, click the Save button to save the settings and create the EVC service request.

**Step 8** Now you are ready to deploy both service requests, see Deploying Service Requests.

# L2VPN/EVC/TDM-CEM/ATM New Features

This section summarizes features that were added to enhance the EVC pseudowire services in Prime Provisioning 6.4.1:

### Setting the MTU Size in an EVC Pseudowire Service

Using Prime Provisioning you can set the maximum transmission unit (MTU) for an EVC pseudowire service. This MTU indicates the MTU which must be configured identically at both ends of the pseudowire for the pseudowire to work. The MTU attribute can be set during EVC policy creation and if set to editable, it can further be edited during service request creation as well.

To set the MTU size using the Prime Provisioning GUI:

1. Navigate to **Service Design > Policy Manager > Create > Policy Type: EVC**.
2. In the Service Option section, enter the maximum transmission unit in the **MTU:** field.
3. Make the required changes and save the EVC policy.

When you look at the configlet generated for this service, you will notice that as a prerequisite Prime Provisioning configures the MTU first under the interface and then under the xconnect. If an MTU value is not specified, the default MTU values that are set on the device are used. This is to ensure that the port has an MTU at least as large as any service it is carrying.

The MTU includes VLAN headers transported over the pseudowire. It does not include the size of the Ethernet header. While the specified MTU value can be configured on IOS devices, an interface MTU is configured in case of IOS-XR devices. The interface MTU is automatically determined by Prime Provisioning based on the size of the Ethernet header and the number of VLAN tags that are pushed or popped. The formula used to compute the interface MTU is,

interface_mtu = pw_mtu + 14 + 4 x tags popped - 4 x tags pushed.

For example if you set the MTU size to 1500, and you have an IOS-XR device on one side of the pseudowire where you match 2 tags and pop 1 tag, then the interface MTU provisioned on the IOS-XR device is 1518 (which is 1500 + 14 + 4 x 1).

This feature is supported through the GUI and the NBI.

### Provisioning a Pseudowire with U-PE Role Based Devices

While creating EVC-Ethernet services you can now provision a pseudowire on U-PE role based devices.

This enables a network architecture that has ethernet access domains, but allows for MPLS enabled switches within those domains. As a prerequisite it is assumed that one VLAN will be set up to carry all the MPLS traffic in that domain. This will then enable end-to-end MPLS based services without having to allocate service provider VLANs, but will allow MPLS enabled access to be inserted within existing ethernet access rings with non-MPLS enabled devices. In earlier Prime Provisioning releases, you could configure MPLS services on provider devices with only the N-PE role. However, starting in Prime Provisioning 6.4.1, Prime Provisioning checks whether in the PE device inventory the Loopback interface giving the LDP ID of the device is defined. If the LDP Loopback ID is defined, the device can be used as an endpoint for an MPLS service.

While creating Access Domain and Interface Access Domain, when you select devices as PEs, a new **Role** column displays the roles of the listed devices. You can also separate out devices based on their role type by using the **Show PEs with Role** filter option.

This support for U-PE and PE-AGG devices is extended to EVC Service Request creation and Multi segment Pseudowire functionality as well.

When you are creating an EVC service request, in addition to provisioning N-PE devices you can now provision MPLS enabled devices of role type U-PE and PE-AGG.

This feature is supported through the GUI and the NBI.

**Template Support for MPLS-Enabled Nodes:**
Prime Provisioning provides template support for N-PE role-based policies when an MPLS node is enabled in a direct connected link. Similarly, template support is provided for U-PE or PE-AGG devices, when a MPLS node is enabled in layer 2 links. But when a device is not enabled with an MPLS node, then no template is attached to the devices.

**Support for Multi Segment Pseudowire:**
In multi segment pseudowire, a filter is created during tunnel creation that displays all the MPLS-enabled devices. It allows the picker in the filter to populate all the MPLS-enabled devices such as U-PE with Loopback or N-PE with Loopback.

### Configuring Speed and Duplex for Devices Added in Direct Connect Links

Using Prime Provisioning, you can now configure the speed and duplex attributes for the EVC UNI enabled on both N-PE and U-PE role based devices added in Direct Connected Links. In addition to setting these attributes for links with L2 access, starting in Prime Provisioning 6.4.1, you can also set the speed and duplex attributes for Direct Connected links.

To set these attributes on devices added in Direct Connected Links:

1. Enable DCPL properties as shown below:
   - Select **Administration** > **Hosts**.
   - Select an appropriate **Host name** and click **Config**.
   - From the **Properties** folder, select **Provisioning > Service > fsm-UNI_DirectConnect > SpeedDuplex**.
   - Set the property value to **True**. By default this DCPL property is set to False.
2. Select a device in a Direct Connected Link.
3. Click **Edit** (Link Attributes).

The Link Speed and Link Duplex attributes can be set in the UNI Information section of the displayed page. The attributes are optional. The values for Link Speed are None, 10, 100, 1000, and Auto. The values for the Link Duplex attribute are None, Full, Half, and Auto.

This feature is supported through the GUI and the NBI.

### VPLS Support on CPT Devices

In Prime Provisioning, when you create a service request for a EVC-VPLS policy, **N-PE Pseudowire on SVI** attribute is enabled and greyed out by default. Even though the attribute **N-PE Pseudowire on SVI** is irrelevant to CPT and ASR903 platforms, this feature helps generate proper CLI's for CPT and ASR903 devices without any user intervention.

### Additional Attributes to Define Pseudowire Classes:

Using Prime Provisioning, you can now provision an EVC service with the following new pseudowire class attributes. These attributes are optional and are supported through both GUI and NBI.

- Control Word: This attribute generates the cli ‘control-word’ under the pw-class.
- Sequencing: Specifies the direction in which sequencing of data packets in the pseudo wire is enabled. The values are:
  - BOTH: Configures sequencing on receive and transmit.
  - RECEIVE: Configures sequencing on receive.
  - TRANSMIT: Configures sequencing on transmit
- Sequencing Resync: Specifies the resync value and the threshold. For example, for a resync value of 200, if the sequence type is Transmit, then the CLI generated under the pw-class for this attribute is “sequencing transmit resync 200 resync threshold”. The range for the sequencing resync is from 5 to 65535.

- Tunnel type – Specifies the type of the tunnel. The values are None, TE, and TP.

For steps on how to create a pseudowire class and specify these attributes, see Creating a Pseudowire Class.

# MPLS VPN New Features

This section summarizes features that were added to enhance MPLS VPN services in Prime Provisioning 6.4.1.

## Duplicating U-PE Values at the PE

This enhancement is for cases where the customer facing interface is on an Ethernet Accesss switch provisioned using 'service instance'.

In Prime Provisioning 6.4 when configuring an access circuit with Ethernet access, you were required to enter match criteria at the U-PE, VLAN rewrites at the U-PE, match criteria at the N-PE, and then execute further rewrites. Since the values matched at the N-PE can be determined by what is matched and rewritten at the U-PE, it is now no longer required to enter these values repeatedly.

The provisioning logic has also been changed such that on the uplink of an Ethernet switch we always pop the service provider VLAN. This is taken into account when determining the configuration of the switch. For example if the rewrite required at the U-PE is to replace the customer VLAN with the provider VLAN, then this is achieved by popping the customer VLAN at the ingress on the customer interface , and pushing the service provider VLAN at egress on the uplink port.

## Updating Device Interface Table Automatically

Prime Provisioning will automatically update the latest pseudowire headend interfaces in the Device Interface table as soon as the service request is saved. This means that the interfaces can be immediately associated with the service configuration before it is deployed.

In earlier Prime Provisioning releases, the created virtual interfaces were updated in the Device Interface table only after successful deployment of the services they were associated with and after a Config Collect was performed. But starting 6.4.1, since this list is updated automatically, you no longer have to manually perform a Collect Configuration for the pw-ether interfaces to be added to the Device Interface list.

This feature is supported through both the GUI and the NBI.

## Configure Router Static and BFD Commands

Using Prime Provisioning 6.4.1, you can enable BFD properties for PE-CE and PE-no-CE policies during Service Request creation. The **BFD required** attribute is enabled only when the Next Hop option is set to **USE_NEXT_HOP_IPADDR** or **OUTGOING_INTF_NAME and NEXT_HOP_IPADDR**. When the BFD required attribute is enabled, the following fields are displayed: BFD Minimum interval, BFD Multiplier.

These attributes are applicable to IOS and IOS-XR devices. During service provisioning, Prime Provisioning ensures that the configlets are generated only for IOS-XR devices.

BFD configlets is generated only if you provide value for "Advertised Routes for CE" attribute. Without this value configlets will not be generated, even if BFD check box is enabled and values for BFD Minimum interval and Multiplier are given. In the generated configlet, the BFD command is generated along with the route command and it is appended with advertised routes for CE. The new attributes that appear in the configlet:

- BFD Required
- BFD Minimum Interval
- BFD Multiplier.

This feature is applicable to IPV4 and IPV6 devices and is supported only through GUI.

# Installation Notes

Prime Provisioning patches are available at:

http://software.cisco.com/download/type.html?mdfid=284586808&flowid=37682

This section contains the following information:



## Version Supported

You can install Prime Provisioning 6.4.1 on Prime Provisioning 6.4 or 6.4.0.1 based server. Schema upgrade is supported from 6.2.1.50/ 6.3.0.3/ 6.4/ 6.4.0.1/ 6.4.0.2 to 6.4.1.

Prime Provisioning 6.4.1 is a maintenance release on the Prime Provisioning 6.4 release. Therefore, repository migration can only be performed from 6.4 or later versions. To migrate from earlier releases (prior to 6.4), you must first upgrade to Prime Provisioning 6.4 release. See "Prime Provisioning 6.4.1 Patch Installation" section on page 15.

The procedure for upgrading from earlier releases is documented in the *Cisco Prime Provisioning 6.4 Installation Guide*.

**Caution** In addition to the privileges mentioned in Prime Oracle User Account section of *Cisco Prime Provisioning 6.4 Installation Guide*, you need to grant one more privilege to Oracle DB user using the below query before executing upgrade tool.
**GRANT SELECT ON sys.dba_constraints TO <<*PRIME PROVISIONING Oracle DB username*>>**

This is applicable only for the Customers who use Oracle Database with Prime Provisioning installation and not for those who use Sybase repository with Prime Provisioning installation.

**Note** The upgrade tool needs to be executed after installing the patch on database schema upgrade. For information on using this tool, see "Using the Upgrade Tool for Schema Upgrade" section on page 19. But when you install 6.4.0.2 patch on 6.4.0.1, you need not use the upgrade tool as there is no change in the schema level.

# Prime Provisioning 6.4.1 Patch Installation

The following sections describes about the **common steps** for the scenarios included for Prime Provisioning 6.4.1 installation in standalone and suite mode:

- 6.4.0.1/ 6.4.0.2 to 6.4.1 Standalone or Suite Mode Installation
- 6.2.1.50/ 6.3.0.3 to 6.4.1 Standalone or Suite Mode Installation
- 6.4 to 6.4.1 Standalone or Suite Mode Installation

The following section describes about the steps required for Suite Mode installation.

- 6.4/ 6.4.0.1/ 6.4.0.2 to 6.4.1 Suite Mode Installation

## 6.4.0.1/ 6.4.0.2 to 6.4.1 Standalone or Suite Mode Installation

To install Prime Provisioning 6.4.1 maintenance path in Standalone mode or Suite mode, follow these steps:

**Note** Prior to installing Prime Provisioning 6.4.1, if you are moving a repository from one machine to another, the schema upgrade fails unless the repository has been initialized on the new machine. This requires that you successfully run **initdb.sh** on the repository to update the host entry. To run **initdb.sh,** execute the command**: $PRIMEP_HOME/ prime.sh initdb.sh.**

**Step 1** Before proceeding to install the Prime Provisioning 6.4.1 Maintenance Release, be sure to back up your repository, as explained in Backup and Restore of Prime Provisioning Repository.

**Step 2** Retrieve the Prime Provisioning 6.4.1 Maintenance Release (**prime_provisioning_641_patch.tar.gz**) from here:

http://software.cisco.com/download/type.html?mdfid=284586808&flowid=37682

**Note** If you have difficulties accessing the software from this location, please go to Cisco.com and choose **Support > Downloads > Cloud and Systems Management > Routing and Switching Management > Fullfillment Products > Cisco Prime Provisioning**.

**Note** You should place the retrieved tar file in a directory outside of the **$PRIMEP_HOME** directory structure.

**Step 3** Prior to installing the Prime Provisioning 6.4.1 maintenance release, verify that you have 100 MB of free space in the **$PRIMEP_HOME** directory and that you are logged in with the same username as the owner of your supported version of Prime Provisioning.

**Step 4** Navigate to the directory, where the Prime Provisioning 6.4.1 Maintenance Release is placed.

**Step 5** Use the following command to untar or unzip **prime_provisioning_641_patch.tar.gz**:

**gunzip -c prime_provisioning_6_4_1_patch.tar.gz | tar xvf –**

**Step 6** If Prime Provisioning is running, use the following command to stop the database, name server, and WatchDog on the machine on which it is running:

**$PRIMEP_HOME/prime.sh stopall**

**Note** To check if Prime Provisioning is running, use the **<PRIMEP_HOME>/prime.sh status** command.

**Step 7** Use the following command to run the patch installation script:

**./primepatchinstall**

You will be prompted with the following message "Enter a new path or press **Enter** for the default **[<*PRIMEP_OWNER_HOME_DIR*>/primep-6.4.1]:".**

**Step 8** To specify the path, where the patch has to be installed, follow the below steps:

a. Press **Enter,** if you want to accept the default path.

b. Enter the path, where the prime has already been installed.

c. To terminate the installer at any time, press **Ctrl-C**.

**Step 9** At the end of the installation, you will get the following message:

```
"Do you want to continue the installation in Standalone mode?"
```

Enter **yes** to finish the installation in standalone mode. This completes the installation process and the installation stops immediately.

**Step 10** If you want to install Prime Provisioning 6.4.1 in suite mode, enter **no** and follow the steps mentioned in the procedure 6.4/ 6.4.0.1/ 6.4.0.2 to 6.4.1 Suite Mode Installation.

**Note** You must execute the upgrade tool before restarting the server. For detailed steps to upgrade, see the "Using the Upgrade Tool for Schema Upgrade" section on page 19.

**Step 11** Navigate to **$PRIMEP_HOME.**

**Step 12** Enter the **$PRIMEP_HOME/prime.sh start** command to restart Prime Provisioning.

## 6.2.1.50/ 6.3.0.3 to 6.4.1 Standalone or Suite Mode Installation

To install Prime Provisioning 6.4.1 maintenance path in Standalone mode or Suite mode follow these steps:

**Step 1** Perform Prime Provisioning 6.4 GUI installation on 6.2.1.50/ 6.3.0.3.

**Step 2** During Prime Provisioning 6.4 installation, provide the same home directory ($PRIMEP_HOME) as used in 6.2.1.50/ 6.3.0.3 installation and choose the **Keep Existing Repository** option.

**Step 3** Once Prime Provisioning 6.4 is complete, perform from Step 2 mentioned in the procedure 6.4 to 6.4.1 Standalone or Suite Mode Installation.

## 6.4 to 6.4.1 Standalone or Suite Mode Installation

To install Prime Provisioning 6.4.1 maintenance path in Standalone mode or Suite mode follow these steps:

**Step 1** During Prime Provisioning 6.4.1 installation, provide the same home directory ($PRIMEP_HOME) as used in 6.4 installation and choose the **Upgrade Existing Repository** option.

**Step 2** Apply the patch to upgrade to 6.4.1.

**Note** Prior to installing Prime Provisioning 6.4.1, if you are moving a repository from one machine to another, the schema upgrade fails unless the repository has been initialized on the new machine. This requires that you successfully run **initdb.sh** on the repository to update the host entry. To run **initdb.sh,** execute the command**: $PRIMEP_HOME/ prime.sh initdb.sh.**

**Step 3** Before proceeding to install Prime Provisioning 6.4.1, ensure that you take a back up of your repository, as explained in Backup and Restore of Prime Provisioning Repository.

**Step 4** Retrieve the Prime Provisioning 6.4.1 software (**prime_provisioning_641_patch.tar.gz**) from here:

http://software.cisco.com/download/type.html?mdfid=284586808&flowid=37682

**Note** If you have difficulties accessing the software from this location, please go to Cisco.com and choose **Support > Downloads > Cloud and Systems Management > Routing and Switching Management > Fullfillment Products > Cisco Prime Provisioning**.

**Note** You should place the retrieved tar file in a directory outside of the **$PRIMEP_HOME** directory structure.

**Step 5** Before you install Prime Provisioning 6.4.1, verify that you have 100 MB of free space in the **$PRIMEP_HOME** directory and that you are logged in with the same username as the owner of your supported version of Prime Provisioning.

**Step 6** Navigate to the directory where the Prime Provisioning 6.4.1 software is downloaded.

**Step 7** Untar (unzip) the software **prime_provisioning_641_patch.tar.gz** using the command:

**gunzip -c prime_proviosioning_6_4_1_patch.tar.gz | tar xvf –**

**Step 8** If Prime Provisioning is running, use the following command to stop the database, name server, and WatchDog on the machine on which it is running:

**$PRIMEP_HOME/prime.sh stopall**

**Note** To check if Prime Provisioning is running, use the **<PRIMEP_HOME>/prime.sh status** command.

**Step 9** Use the following command to run the patch installation script:

**./primepatchinstall**

You will be prompted with the following message “Enter a new path or press **Enter** for the default **[***<PRIMEP_OWNER_HOME_DIR>***/primep-6.4.1]:”.**

**Step 10** To specify the path, where the patch has to be installed, follow the below steps:

**a.** Press **Enter,** if you want to accept the default path.

**b.** Enter the path, where the prime has already been installed.

**c.** To terminate the installer at any time, press **Ctrl-C**.

**Step 11** At the end of the installation, you will get the following message:

```
"Do you want to continue the installation in Standalone mode?"
```

Enter **yes** to finish the installation. This completes the installation process and the installation stops immediately.

**Step 12** If you want to install Prime Provisioning 6.4.1 in suite mode, enter **no** and follow the steps mentioned in the procedure 6.4/ 6.4.0.1/ 6.4.0.2 to 6.4.1 Suite Mode Installation.

**Note** You must execute the upgrade tool before restarting the server. For detailed steps to upgrade, see "Using the Upgrade Tool for Schema Upgrade" section on page 19.

**Step 13** Navigate to **$PRIMEP_HOME.**

**Step 14** Enter the **$PRIMEP_HOME/prime.sh start** command to restart Prime Provisioning.

## 6.4/ 6.4.0.1/ 6.4.0.2 to 6.4.1 Suite Mode Installation

To continue installing the Prime Provisioning 6.4.1 maintenance patch in suite mode, follow these steps:

**Step 1** During patch installation, if Prime Provisioning 6.4 is installed in suite mode, you will get the following message:

```
"Please remove the already registered Prime Provisioning server from Prime Central
i.e. From Prime Central Suite monitoring Portlet, remove Prime Provisioning."
```

**Note** This message ensures that already registered Prime Provisioning server is removed from Prime Central Suite monitoring Portlet. The necessary steps are documented here: http://www.cisco.com/en/US/docs/net_mgmt/prime/central/1.0/user/guide/prime_central_10_user_guide_suite_mgmt.html#wp1057447

To terminate the patch installation in suite mode, enter **no**.

**Step 2** Enter **yes** to continue with suite mode installation.

**Step 3** Enter the following details about the Prime Central database on prompt:

- Server IP Address- IP Address of the Prime Central Database server
- SID- Server instance identifier of the Prime Central Database server
- Port- Port number of the Prime Central Database server
- DB User- Database username of the Prime Central Database server
- DB Password- Database password associated with the above username.

**Note** While 6.4.1 patch installation, you will get a warning message on **DCS.IOSWarningExpressions**, which can be ignored.You must execute the upgrade tool before restarting the server. For detailed steps to upgrade, see "Using the Upgrade Tool for Schema Upgrade" section on page 19.

**Step 4** Navigate to **$PRIMEP_HOME.**

**Step 5** Enter the **$PRIMEP_HOME/prime.sh start** command to restart Prime Provisioning.

**Note** Restart integration layer on Prime Central after suite mode installation. Instructions for how to do this are found here: http://www.cisco.com/en/US/partner/docs/net_mgmt/prime/central/1.1/user/guide/prime_central_11_user_guide.html

# Using the Upgrade Tool for Schema Upgrade

The following steps describe how to use the upgrade tool to update the database schema. To upgrade the schema from other versions of Prime Provisioning to Prime Provisioning 6.4.1, follow these steps:

**Step 1** Copy the upgrade tool from the image location to any preferred location. For example:

**cp prime_provisioning_641_upgradeTool.tar.gz /opt/**

**Step 2** Use the following command to untar or unzip **prime_provisioning_641_upgradeTool.tar.gz**:

**gunzip -c prime_provisioning_641_upgradeTool.tar.gz | tar xvf –**

**Step 3** Unzip the file isc-upgrade.zip to extract its contents:

**unzip isc-upgrade.zip**

**Step 4** Go to the **upgradeTool** folder and execute the following command to run the upgrade tool:

**$ ./upgradeISCSchema.sh $PRIMEP_HOME**

**Step 5** Provide the admin credentials on prompt to continue with the upgrade tool installation.

```
Please enter ISC admin user name [admin]:
Please enter admin password:
Please enter admin password again:
```

# Uninstall

To uninstall the Prime Provisioning 6.4.1 maintenance release that was successfully installed, follow these steps:

**Step 1** Log in with the same username as the owner of Prime Provisioning 6.4.1.

**Step 2** Navigate to the **$PRIME_HOME** directory.

**Step 3** If Prime Provisioning 6.4.1 is running, use the following command to stop the database, name server, and WatchDog on the machine on which it is running:

**$ ./prime.sh stopall**

**Step 4** Navigate to the directory **$PRIMEP_HOME/patch/prime6.4.1-patch-08**, where all the files replaced by the Prime Provisioning 6.4.1 maintenance release were stored.

**Step 5** Use the following command to run the patch script to uninstall:

$ **./primepatchrollback**

a. When you run this script, you are asked to ensure that you have followed the equivalent of **Step 1** and **Step 2**.

b. To accept the default value for a prompt indicated in **[ ]**, for example, **[n]** or **[y]**, press **Enter**. To terminate the installer at any time, press **Ctrl-C**.

c. You are asked if you would like to roll back the patch. Answer yes or no as prompted.

d. At the end of the uninstall, you receive a message that the patch rollback is complete.

**Step 6** Navigate to **$PRIMEP_HOME.**

**Step 7** Enter the **./prime.sh start** command to restart Prime Provisioning.

**Note** You can only restart Prime Provisioning if you restore a copy of the backed up repository from the version of the patch used prior to the Prime Provisioning 6.4.1 upgrade.

# Prime Provisioning 6.4.1 Resolved Bugs

Customer-found bugs that have been fixed in the Prime Provisioning 6.4.1 release are indicated in the following table. This includes Prime Provisioning bugs from the Prime Provisioning 6.4.0.1 release.

| Bug ID | Description |
|---|---|
| CSCud63883 | DCPL attribute description has wrong spelling for ForceTemplateDeploy. |
| CSCud64189 | CreatePE.xml,role type default value should show as N-PE instead of N_PE. |
| CSCud68798 | Customer site GUI Edit page is showing "Internal error”. |
| CSCud95281 | Template modification modifies the auto picked VlanID. |
| CSCue01707 | IE 9 becomes unresponsive while trying to list all the interfaces in device screen. |
| CSCue46289 | PP remove mtu size cmd pushed through template on modification. |
| CSCue48371 | IPRAN-ATM Service on ASR9K - subinterface is not mandatory. |
| CSCue50527 | Set auto pick for outer vlan field, but the vlan field is still editable. |
| CSCue53251 | Inventory Import is importing incorrect or blank device credentials. |
| CSCue55291 | Tasklogs do not refresh. |
| CSCue55339 | EVC - CEM class does not align properly in policy. |
| CSCue55403 | EVC - CEM-class need option 'None' for Dummy Mode. |
| CSCuf93848 | PP- Typo on EVC Local Link error message. |
| CSCuf35387 | VCID is not picked properly while creating EVC SR. |
| CSCuf52079 | NBI response for Service on FAILED state returns faulty/No Log Content. |
| CSCuf89875 | MSPW-deployment goes to failed audit on multiple neighbor. |

| Bug ID | Description |
|---|---|
| CSCuf55033 | SR goes to failed Audit on modification when outervlan range is used. |
| CSCue82061 | CPE Hostname query for 'ALL'/'VPLS' option is listing incorrect services. |
| CSCue48401 | EVC - VCid values are not retained. |
| CSCuf56383 | Modifying EVC SR to uncheck pop outer tag is not removing rewrite config. |
| CSCue55156 | Decommission of EVC-VPLS service is not removing the config. |
| CSCue84009 | PW-class is not removed after decommission using MSW EVC/VPLS SR. |
| CSCuf47071 | Wrong config matching untagged at ME-3600 U-PE. |
| CSCuf35550 | TE discovery fails to discover strict path that uses loopback i/f. |
| CSCue58238 | User group selection is not clearing from screen on new user creation. |
| CSCue96524 | Grey Mgmt route-policy provisioning on IOSXR fails because of the 64 char limit. |
| CSCuf83237 | PP- Unable to create MPLS SR with NPC. |
| CSCuf61087 | SR moves to failed audit state during decommission. |
| CSCtg37389 | Vlan pool is not releasing properly. |
| CSCud80089 | Natively supported commands deleted from device during SR modification. |
| CSCug02739 | NBI SR Deploy with future time set is triggering the task continuously. |

# Prime Provisioning 6.4.1 Open Bugs

The following open bugs apply to Prime Provisioning 6.4.1:

| BUG ID | Description |
|---|---|
| CSCue54748 | PP should not allow you to modify Labels in attributes. |
| CSCue82712 | Multiple commit-sessions within an SR execution cycle. |
| CSCue84087 | Error message of Inner VLAN ID is showing wrong in GUI/NBI. |
| CSCuf21231 | Proper Task log error has to be thrown for invalid SRs. |
| CSCuf47133 | Modification of EVC Local SR goes to failed deployed state. |
| CSCuf60746 | Customized Template Boundary values should be validated within that page. |
| CSCuf60878 | Customization files are not retained in the product. |
| CSCuf65348 | The tasklog goes to internal error for failed HVPLS SR. |
| CSCuf84144 | EVC syx inL2:RewriteActionType Translate should not display 2:1 and 2:2 in GUI. |
| CSCug37205 | TE Full Discovery failed with SQL Exception error. |
| CSCug28723 | NBI throws error when Interface id is given its max range-PWHeadEnd. |
| CSCug28831 | Validation error in Eigrp protocol attributes-PWHeadEnd. |
| CSCug79484 | MPLS PW SR goes to Failed_Audit in XR V 4.3.1.30I. |

| BUG ID | Description |
|---|---|
| CSCug71219 | EVC - AD should not be mandatory for EVC service. |
| CSCug21832 | NBI: Not generating Negate cmd for modify DIO and Maxprefix in BGP. |
| CSCug79080 | EVC - sorting by customer column throws error. |
| CSCug81650 | EVC - Pw-class name modification does not subsume the associated SR/Policy. |
| CSCug81529 | EVC - Tunnel type “none” should be present in pw class inventory. |
| CSCug58764 | PP should not allow to save EVC-PW SR with VLAN range and POP in UPE. |
| CSCug84817 | PP- Device Column Sort not working for TEM Seed Router Discovery. |
| CSCug76061 | Saving no-changes to SR created by NBI throw exception. |
| CSCug10415 | PE-CE Intf Addr pg is invisible when temp is added with autopick ip addr. |
| CSCug83439 | Suppression of "switchport trunk encapsulation dot1q". |
| CSCug76371 | PP throws SQL Excep Err, while saving L2 Access link with encp untagged. |
| CSCug10300 | EVC-VPLS-MS SR,GUI and NBI tasklog mismatch. |
| CSCug81668 | PW-Class attribute set non-editable becomes editable in ATM SR. |
| CSCtz55666 | Static VPLS SR page alignment not proper. |
| CSCug69093 | EVC syntax: PP should take appropriate values for SI id for manual/auto. |
| CSCug75922 | BDI interface is displayed as VLAN for ASR903. |
| CSCug58605 | EVC- local Sr goes to failed audit IOS-XR 4.3.1. |
| CSCug83900 | Restoring the live backup fails in vimto BR Tool. |
| CSCug83879 | EVC-XConnect-MTU-not retaining changed value after modifying link attributes. |
| CSCug18532 | Duplicate entry of customized template attribute in IPRAN ATM Policy. |
| CSCug07244 | EVC-VPLS SR with direct non flex links goes to failed_deploy state. |
| CSCug91613 | Negate for RD/RT during modify multicast VPN in IOS6VPE/XR not generated. |
| CSCug88808 | EVC - Static Single Segment pw requires path xml. |

# Finding Known Problems in Prime Provisioning 6.4.1

To find known problems in Prime Provisioning 6.4.1, use the following URL:

http://tools.cisco.com/Support/Bug Tool Kit

You must log into Cisco.com.

You can search for specific bugs or search for a range by product name. This tool enables you to query for keywords, severity, range, or version.

Use the following search criteria to locate bugs for Prime Provisioning 6.4.1:

- Product category: **Cloud and Systems Management.**
- Product: **Cisco IP Solution Center or Cisco Prime Fulfillment or Cisco Prime Provisioning**
- Software version: **6.4.1** (For a list of bugs open against all releases, choose **ANY**.)

The results display bug ID and title, found-in version, fixed-in version, and status. The bug ID is a hyperlink to detailed information for the bug ID's product, component, severity, first found-in, and release notes.

The results could be displayed in a feature matrix or spreadsheet.

# Related Documentation

The entire documentation set for Prime Provisioning, can be accessed at:

http://www.cisco.com/en/US/products/ps12199/tsd_products_support_series_home.html

An overview of the Cisco Prime Provisioning product is available at:

http://www.cisco.com/go/provisioning

The following documents comprise the Prime Provisioning 6.4 documentation set:

### General Documentation (in suggested reading order)

- *Cisco Prime Provisioning 6.4 Documentation Overview*
- *Cisco Prime Provisioning 6.4 Installation Guide*
- *Cisco Prime Provisioning 6.4 Supported Devices*
- *Cisco Prime Provisioning 6.4 User Guide*
- *Cisco Prime Provisioning 6.4 Administration Guide*
- *Cisco Prime Provisioning 6.4 Open Source*

### API Documentation

- *Cisco Prime Provisioning 6.4 API Programmer Guide*
- *Cisco Prime Provisioning 6.4 API Programmer Reference*

**Note** All documentation *might* be upgraded over time. All upgraded documentation will be available at the same URLs specified in this document.

### Other Cisco Prime Product Documentation

See also the documentation for the following Cisco Prime products:

- *Cisco Prime Central*
- *Cisco Prime Network*
- *Cisco Prime Optical*
- *Cisco Prime Performance Manager*

# Accessibility Features in Prime Provisioning

For a list of accessibility features in Prime Provisioning, visit Cisco's Voluntary Product Accessibility Template (VPAT) website, or contact accessibility@cisco.com.

All product documents are accessible except for images, graphics and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

---