



CHAPTER 58

Getting Started

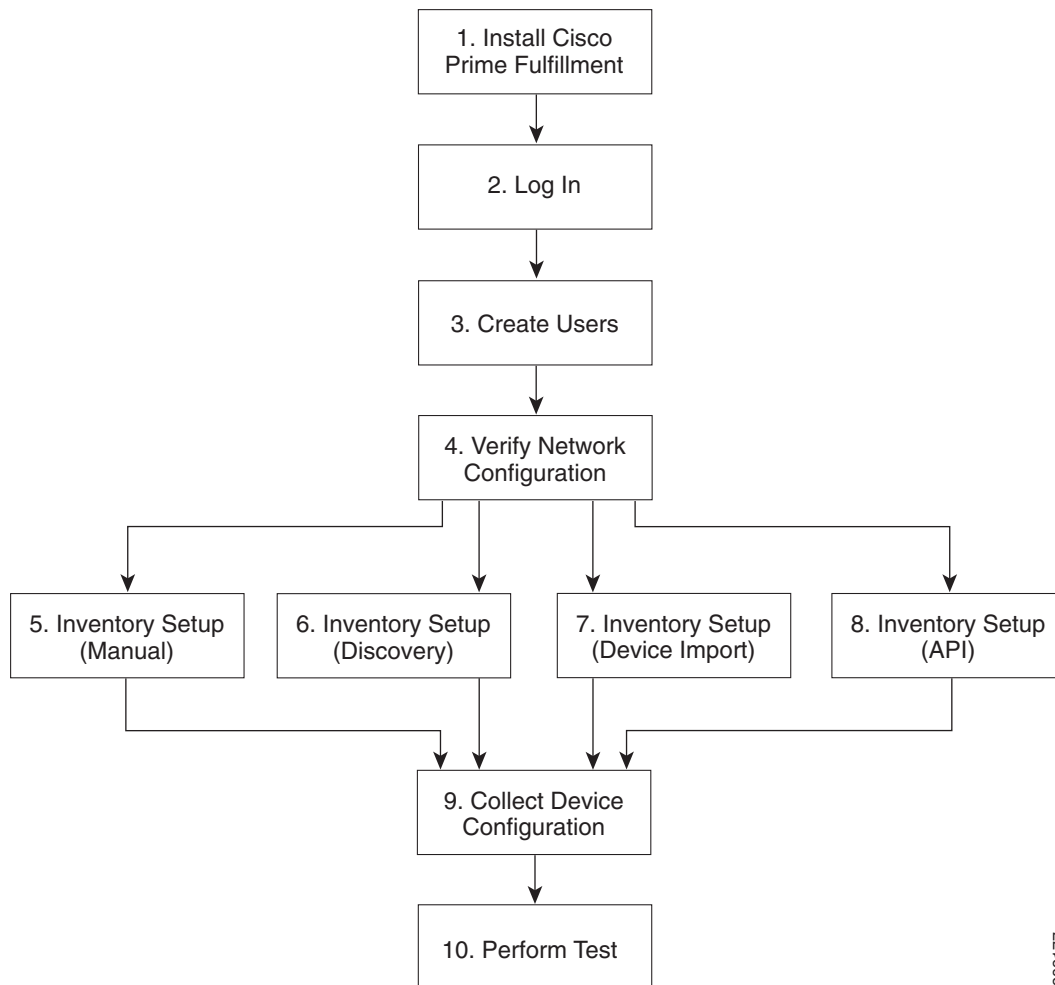
This chapter describes how to get started using Cisco Prime Fulfillment Diagnostics.

This chapter contains the following sections:

- [User Roles, page 58-3](#)
- [User Roles, page 58-3](#)
- [Creating Users, page 58-3](#)
- [Network Configuration, page 58-3](#)
- [Inventory Setup, page 58-4](#)

[Figure 58-1](#) describes the getting started workflow for Prime Diagnostics.

Figure 58-1 Getting Started with Prime Diagnostics



282177

1. Create Users—Create users and assign Diagnostics user roles. See [User Roles, page 58-3](#), and [Creating Users, page 58-3](#).
2. Verify Network Configuration—Verify that all network devices have the configuration required for Diagnostics. See [Network Configuration, page 58-3](#).
3. Inventory Setup (Manual)—Manually create required Prime Fulfillment inventory objects. See [Inventory Setup, page 58-4](#).
4. Inventory Setup (Discovery)—Create required Prime Fulfillment inventory objects using Prime Fulfillment Discovery. See [Inventory Setup, page 58-4](#).
5. Inventory Setup (Device Import)—Create required Prime Fulfillment inventory objects using Inventory Manager Import Devices feature. See [Inventory Setup, page 58-4](#).
6. Inventory Setup (API)—Create required inventory objects through Prime Fulfillment APIs. See [Inventory Setup, page 58-4](#).
7. Collect Device Configuration—Collect device configuration, including interface configuration, and add to Prime Fulfillment inventory. A scheduled task can be set up to periodically synchronize Prime Fulfillment inventory with actual device configuration. See [Device Configuration Collection, page 58-8](#).

8. Perform Test—Select, configure, and run an MPLS VPN Connectivity Verification test. See [Chapter 59, “Performing an MPLS VPN Connectivity Verification Test”](#).

User Roles

The functionality available to you as an Prime Fulfillment user is determined by your assigned user roles. User roles also allow you to create and delete devices, collect device configuration, and to perform an MPLS VPN Connectivity Verification test.

To use the Diagnostics functionality, you must be assigned one or more of the following predefined Diagnostics roles depending on the type of connectivity tests you are entitled to perform:

1. `MplsDiagnosticsRole`—You can perform an MPLS VPN connectivity test between two CEs.
2. `MplsDiagnosticsPeToAttachedCeTestRole`—You can perform an MPLS VPN connectivity test between a PE and an attached CE.
3. `MplsDiagnosticsCetoPeAcrossCoreTestRole`—You can perform an MPLS VPN connectivity test between a CE and a PE across the MPLS core.
4. `MplsDiagnosticsPetoPeInVrfTestRole`—You can perform an MPLS VPN connectivity test between two PEs.
5. `MplsDiagnosticsPeToPeCoreTestRole`—You can perform a core MPLS connectivity test between two PEs.



Note

All Diagnostics roles allow you to create and delete devices, collect device configuration, and to perform an MPLS VPN Connectivity Verification test.

Creating Users

For details on how to create Prime Fulfillment users, see the [Chapter 70, “Manage Security”](#) chapter.

Network Configuration

This section describes the network configuration required to allow Diagnostics to troubleshoot your network.

MPLS IP Time To Live Propagation

MPLS IP Time To Live (TTL) propagation is enabled by default on Cisco devices. Diagnostics requires that MPLS IP TTL propagation is enabled within the MPLS core. If MPLS IP TTL propagation is not enabled, then Diagnostics is unable to troubleshoot problems within the MPLS core. Troubleshooting of problems in the access circuit, or on the edge of the MPLS core is still possible.

In Cisco IOS, it is possible to disable MPLS IP TTL propagation for packets forwarded to the MPLS core by using the **no mpls ttl-propagate forward** IOS command. This command stops TTL propagation for packets forwarded in to the MPLS core, but allows TTL propagation for packets sent from within the MPLS core. Diagnostics functions correctly in this situation.

When TTL propagation is disabled using the Cisco IOS command **no mpls ip propagate-ttl**, or the Cisco IOS XR command **mpls ip-ttl-propagate disable**, then all TTL propagation is disabled and Diagnostics is unable to troubleshoot your MPLS network.

**Note**

Timestamp must be disabled for the devices, that are selected for troubleshooting and as well as for the devices that are part of the same network.

MPLS LSP Ping/Trace Route Revision

Diagnostics supports IOS MPLS LSP Ping/Traceroute implementations based on version 3 of the IETF LSP Ping draft (draft-ietf-mpls-lsp-ping-03.txt). Later versions of the IETF LSP Ping draft are not supported. Recent IOS versions (including 12.4(6)T), and IOS XR implement later versions of the IETF LSP Ping draft / RFC 4379. To use Diagnostics with these IOS or IOS XR versions you must configure IOS or IOS XR to use version 3 of the IETF LSP Ping draft. To do so you should enter the **mpls oam** command followed by the **echo revision 3** command in IOS or IOS XR global configuration mode. You should ensure that all routers in your core are using the same version of the IETF LSP ping draft or RFC as appropriate.

31-Bit Prefixes on Point-to-Point Access Circuit Links

For Access circuit links that use IPv4 addressing, Diagnostics supports troubleshooting over access circuit links configured with a 31-bit prefix. However, for each classful network, Diagnostics does not support troubleshooting over two possible 31-bit prefix configurations. These are the subnets that use the classful network address or network broadcast address as a host address. For example, in the class A network, 10.0.0.0, the 31-bit prefix subnet that uses the IP addresses 10.0.0.0 and 10.0.0.1 as host addresses, and the subnet that uses the IP addresses 10.255.255.254 and 10.255.255.255 as host addresses, are not supported. All subnets between these ranges are supported.

If a Diagnostics test is configured using an unsupported 31-bit prefix subnet, then the test is not run and a message is displayed informing you of the unsupported 31-bit prefix configuration. In this situation, you must manually troubleshoot this link or reconfigure the link to use a supported subnet configuration.

Inventory Setup

Diagnostics can be used without any dependency on other Prime Fulfillment modules. However, before it can be used, the Prime Fulfillment repository must be populated with a number of objects. As a minimum this includes Provider, Provider Region, Device, and PE Device objects. The role of each of these objects is explained below:

- **Provider**—A Provider is typically a service provider or large corporation that provides network services to a customer. A Provider is a logical inventory object that represents a particular provider.
- **Provider Region**—A Provider Region is considered to be a group of provider edge routers (PEs) within a single Border Gateway Protocol (BGP) autonomous system. The primary objective for defining Provider Regions is to allow a provider to employ unique IP address pools in large Regions, such as Europe, Asia Pacific, and so forth.
- **Device**—A Device in Prime Fulfillment is a logical representation of a physical device in the network. Every network element that Prime Fulfillment manages must be defined as a device in the system.

- PE Device—A PE Device is a logical representation of a Provider Edge (PE) or Provider (P) router that has been associated with a particular Provider Region. A PE Device must first be added as a Device and then assigned a PE Device type.

All Provider Edge (PE) and Provider (P) routers in the MPLS network must be added to the Prime Fulfillment inventory. Each Provider Edge router should be created as a Device and then as a PE Device with a Role Type of N-PE (Network-facing PE). Each Provider device should be created as a Device and then as a PE Device with a role type of P (Provider). Adding customer premises equipment (CPE) devices to the Prime Fulfillment inventory is optional.

**Note**

Where a Device is acting as both a Provider and Provider Edge Device it should be created as a PE Device with a Role Type of N-PE (Network-facing PE).

Many MPLS VPN networks employ a Route Reflector. It is recommended that Route Reflectors should be added to the Prime Fulfillment inventory. A Route Reflector should be added as a Device and then as a PE Device with role type of P. By adding the Route Reflector to the Prime Fulfillment inventory, Diagnostics is able to identify possible failures involving this device.

**Note**

If other Prime Fulfillment features are being used to manage the MPLS network, many of the required inventory objects might already exist. For example, if the Prime Fulfillment MPLS VPN feature is being used, the required Provider, Provider Region, and Provider Edge devices might already exist. In this case only the Provider devices must be added.

A number of options exist for creating the required inventory objects. These objects can be created manually through the Prime Fulfillment GUI, using the Prime Fulfillment Discovery functionality, using the Inventory Manager Import Devices functionality, or using third-party Operations Support System (OSS) client programs that utilize the Prime Fulfillment APIs. Each of these options is described in the following sections:

- [Manual Creation, page 58-5](#)
- [Discovery, page 58-6](#)
- [Inventory Manager Device Import, page 58-7](#)
- [Prime Fulfillment APIs, page 58-7](#)
- [Device Configuration Collection, page 58-8](#)

**Note**

When creating Devices, the Device access information (login and passwords) must match that configured on the physical device.

Manual Creation

Manual creation allows you to add objects to the Prime Fulfillment Repository by entering the required configuration through the Prime Fulfillment Graphical User Interface (GUI). Manual object creation is recommended where a small number of objects are being added to the Prime Fulfillment Repository. The sequence for manual object creation is shown below:

1. Create Provider
2. Create Provider Region
3. Create Devices

4. Collect Device configuration, including interface configuration
5. Create PE Devices, including assigning roles for Provider and Provider Edge devices

**Note**

Both Provider (P) and Provider Edge (PE) devices should be added to the Prime Fulfillment repository as PE Device objects with an appropriate PE Role Type. For details of the PE Role Types that should be assigned to Provider and Provider Edge devices, see [Inventory Setup, page 58-4](#). When selecting the transport mechanism to be used between the Prime Fulfillment server and the device, Cisco CNS Configuration Engine cannot be used with Diagnostics as it does not support the necessary commands that Diagnostics requires. If attempts are made to use Cisco CNS Configuration Engine with Diagnostics, then Diagnostics incorrectly reports that the device cannot be contacted.

For details of how to manually create Provider, Provider Region, Device and PE Device objects, see [Chapter 5, “Setting Up Resources”](#).

When manually creating Devices, you must also add the interface configuration for these devices.

Interface configuration can either be added manually during Device creation, or by using a Task Manager Collect Configuration task. For details of how to perform a Task Manager Collect Configuration task, see [Device Configuration Collection, page 58-8](#). We recommend that you use a Collect Configuration task.

Discovery

Discovery allows you to add the devices in your network to the Prime Fulfillment Repository by configuring minimal device and topology information in XML files. The Discovery process then queries these devices and populates the Prime Fulfillment Repository with the required device and topology information. We recommend that Discovery is used where a large number of objects are being added to the Repository.

Prime Fulfillment Discovery provides two methods for discovering devices: CDP or Device/Topology. Before performing Device Discovery it is necessary to create the required Discovery XML configuration files. For details of how to discover devices, see [Chapter 2, “Inventory - Discovery”](#).

**Note**

Both Provider (P) and Provider Edge (PE) devices should be added to the Prime Fulfillment repository as PE Device objects with an appropriate PE Role Type. For details of the PE Role Types that should be assigned to Provider and Provider Edge devices, see [Inventory Setup, page 58-4](#).

**Note**

After Discovery has completed, you must run a Task Manager Collect Configuration task for all discovered devices. If you do not run a Collect Configuration task, Diagnostics is unable to log in to the discovered devices to perform troubleshooting. For details of how to perform a Task Manager Collect Configuration task, see [Device Configuration Collection, page 58-8](#).

Inventory Manager Device Import

The Inventory Manager Import Devices feature allows you to import multiple devices in to the Prime Fulfillment Repository from files containing the Cisco IOS running configuration of the devices. We recommend that the Inventory Manager Import Devices feature is used where a large number of objects are being added to the Repository. For details of how to import devices, see [Chapter 2, “Inventory - Discovery”](#).

Before importing Provider (P) and Provider Edge (PE) devices you must create the required Provider and Provider Region objects. For details of how to manually create Provider and Provider Region objects, see [Chapter 2, “Inventory - Discovery”](#).

When importing devices you must specify the directory where files containing the Cisco IOS running configuration are located. Do not specify the file names. The files must be located in a file system directory accessible from the Prime Fulfillment server.

**Note**

Both Provider (P) and Provider Edge (PE) devices should be added to the Prime Fulfillment repository as PE Device objects with an appropriate PE Role Type. For details of the PE Role Types that should be assigned to Provider and Provider Edge devices, see [Inventory Setup, page 58-4](#).

**Note**

The enable secret password is encrypted before it is added to the Cisco IOS running configuration. As a result, the Device Import feature is unable to set the enable secret password for devices imported in to the Prime Fulfillment Repository. If the enable secret password is set on any devices being imported, you must manually configure the enable password for these devices in the Prime Fulfillment Repository. If both the enable and enable secret passwords are set for a device, the Inventory Manager Import Devices feature uses the enable password for the device added to the Prime Fulfillment Repository. You must override this password with the correct enable secret password. The enable password for devices in the Prime Fulfillment Repository can be set during or after device import.

**Note**

After Device Import has completed, you must run a Task Manager Collect Configuration task for all imported devices. If you do not run a Collect Configuration task, Diagnostics is unable to log in to the imported devices to perform troubleshooting. For details of how to perform a Task Manager Collect Configuration task, see [Device Configuration Collection, page 58-8](#).

Prime Fulfillment APIs

The Prime Fulfillment application program interface (API) allows you to use operations support system (OSS) client programs to connect to the Prime Fulfillment system. The Prime Fulfillment APIs provide a mechanism for inserting, retrieving, updating, and removing data from Prime Fulfillment servers. It is possible to add the required Provider, Provider Region, Device and PE Device objects using the APIs.

**Note**

The Prime Fulfillment API is not included as standard with Diagnostics, it can be purchased separately.

For details of how to use the Prime Fulfillment APIs, see the [Cisco Prime Fulfillment API Programmer Guide 6.1](#) and the [Cisco Prime Fulfillment API Programmer Reference 6.1](#).

Device Configuration Collection

We recommend that a Task Manager Collect Configuration task is used to add interface configuration to Devices in the Prime Fulfillment Repository. A Task Manager Collect Configuration task connects to the physical device in the network, collects the device information from the router (including interface configuration), and populates the Prime Fulfillment Repository with this information.

For details of how to add Device interface configuration using a Task Manager Collect Configuration task, see [Chapter 52, “Task Manager”](#).

Synchronizing the Prime Fulfillment Repository with Device Configuration

**Note**

The accuracy of Diagnostics is dependent on up-to-date device information. We recommend that the device configuration is resynchronized with the physical devices after any configuration changes and at periodic intervals. This ensures that the device configuration held in the Prime Fulfillment inventory is consistent with the physical devices in the network.

We recommend that device configuration is kept up-to-date using a scheduled Task Manager task. Either Collect Configuration or Collect Configuration from File can be used. For details of how to create a scheduled Task Manager Collect Configuration task, see [Chapter 52, “Task Manager”](#). All PE and P routers in the MPLS network should have their configuration collected using a scheduled Task Manager Collect Configuration task. The Task Manager Collect Configuration task collects details of interface configuration and other device attributes. The interval at which Task Manager Collect Configuration tasks should be scheduled to run depends on the frequency of configuration changes to the network. We recommend running the Task Manager Collect Configuration task daily on each P and PE router.