CHAPTER 42

Administration

A number of administrative features in Cisco Prime Fulfillment Traffic Engineering Management (TEM) are common to Prime Fulfillment. Instructions on how to use these features are described in detail starting in Manage Active Users and User Account, page 67-1.

In this chapter, only TE-specific administrative features are described.

This chapter includes the following sections:

TE User Roles

A TE user role can be a predefined or a user-specified role defining a set of permissions. For a detailed description of user roles in Prime Fulfillment and how to use them, see User Roles, page 70-8.

To access the User Roles window and locate the TE user roles, choose **Administration > Roles**. The User Roles window appears.

There are two pre-defined TEM user roles:

- **TERole**—Grants full permission to TEM operations.
- **TEServiceOpRole**—Grants permission only to manage the TE Admission SR.

TE Policies

Policies are used to define common tunnel attributes. Attributes such as bandwidth pools, hold and setup priority, and affinity bits, are set manually during policy creation as described below.

This section describes the following policy operations:

Create Policy

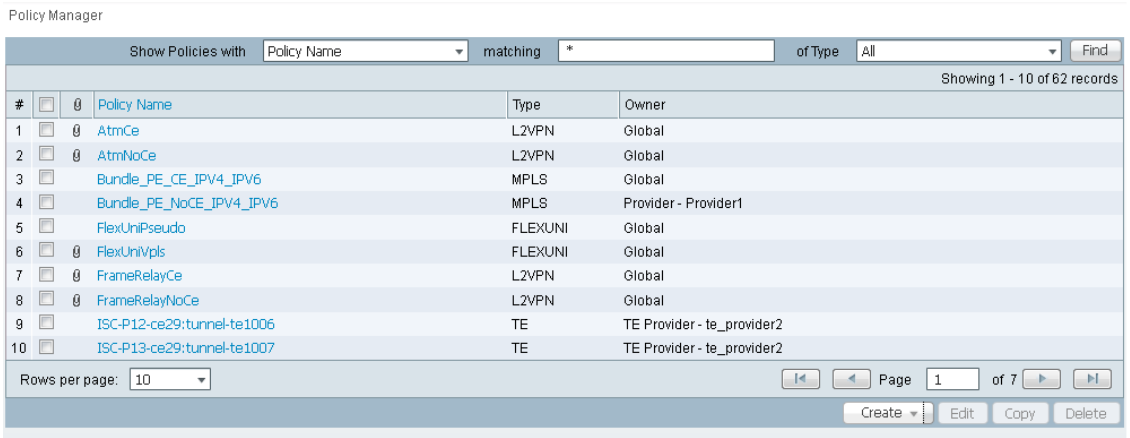
Prime Fulfillment allows you to create TE-specific policies in a manner similar to other policies.

To create a TE policy, use the following steps:

Step 1 Choose **Service Design > Policy Manager**.

The Policy Manager window in Figure 42-1 appears.

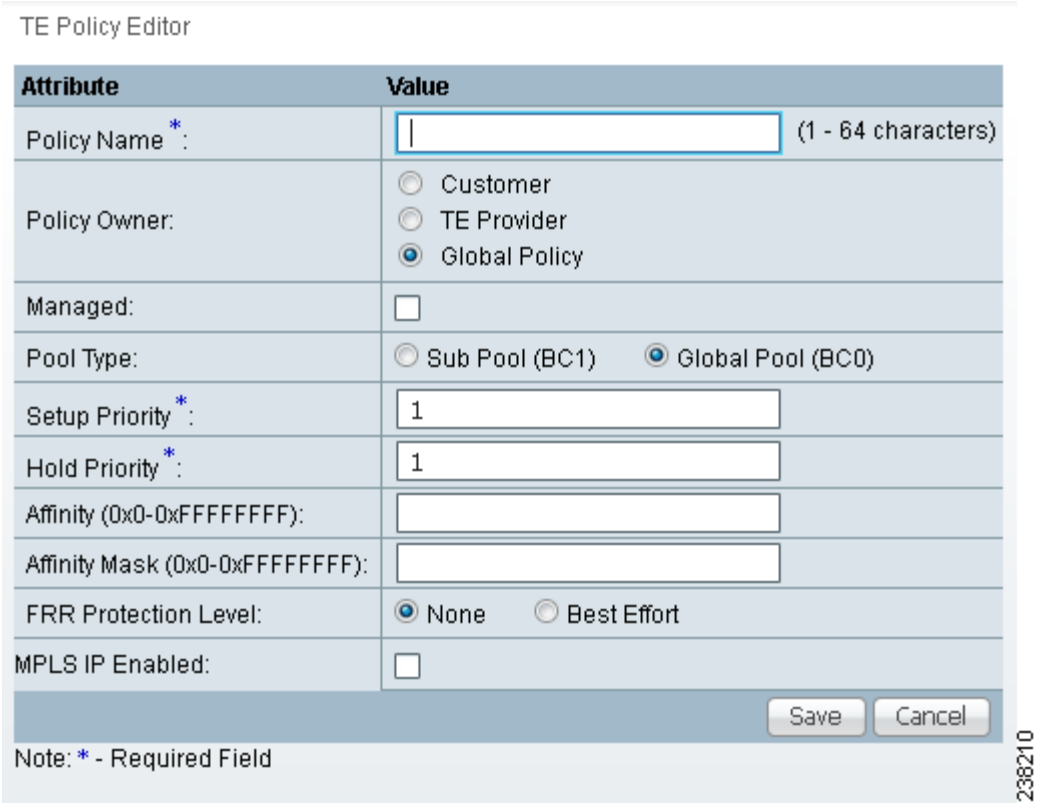
Figure 42-1 Policy Manager



Step 2 Click **Create** and select **TE Policy** to set up a new TE policy.

The TE Policy Editor window in Figure 42-2 appears.

Figure 42-2 TE Policy Editor



The TE Policy Editor window includes the following fields:

- **Policy Name**—Name of the TE policy chosen by the user.
- **Owner**—The owner of the TE policy.
- **Managed**—Check this box to make the policy to be used by managed tunnels. When clicked, both the setup and hold priorities are set to zero and these are not editable. If the box is unchecked, the setup/hold priorities can be set to a value between 1 and 7.

  Clicking the **Managed** check box will add some extra fields in the TE Policy Editor corresponding to two additional protection levels for **FRR Protection Level** (Fast Re-Route) and a new field, **Delay Constraint**.
- **Pool Type**—Tunnel bandwidth pool type for this policy. For a definition of pool types, see the Bandwidth Pools section in the *Cisco Prime Fulfillment Theory of Operations Guide 6.1* .
  - **Sub Pool (BC1)**—Bandwidth will be reserved from Sub Pool.
  - **Global Pool (BC0)**—Bandwidth will be reserved from Global Pool.
- **Setup Priority**—Priority used when signaling an LSP for the tunnel to determine, which of the existing tunnels can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 hold priority.
- **Hold Priority**—Priority associated with an LSP for the tunnel to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.

- **Affinity**—Attribute values required for links carrying the tunnel (bit values are either 0 or 1).
- **Affinity Mask**—Which attribute values should be checked. If a bit in the mask is 0, a link's attribute value of that bit is irrelevant. If a bit in the mask is 1, the link's attribute value and the tunnel's required affinity for that bit must match.
- **FRR Protection Level**—Level of Fast Reroute protection required on the primary tunnel.
  - **None**—No backup tunnel needed.
  - **Best Effort**—Use backup tunnel if available.
  - **Link & SRLG**—Primary tunnel must pass through only links or SRLGs that are FRR-protected
  - **Link, SRLG & Node**—Primary tunnel must pass through only intermediate nodes and links or SRLGs that are FRR-protected.
- **MPLS IP Enabled**—This configures the tunnel with the **mpls ip** command if enabled.

Edit Policy

A policy can be edited only if it is not associated with a tunnel.

To edit a TE policy, use the following steps:

Step 1 Choose **Service Design > Policy Manager**.

The Policies window in Figure 42-2 appears.

Step 2 Select the desired policy and click **Edit**.

The TE Policy Editor window appears. The policy editor is described in Create Policy, page 42-2. The only difference between the create and edit processes is that the policy name and owner are not editable when editing a policy.

Step 3 Make the desired changes to the policy attributes and click **Save**.

If the save operation succeeds, the new TE policy now appears in the Policies window. If not, the **Status** box will indicate the type of error that occurred and, when possible, the corrective action required.

Delete Policy

A policy can be deleted only if it is not associated with a tunnel.

To delete a TE policy, use the following steps:

Step 1 Choose **Service Design > Policy Manager**.

The Policies window in Figure 42-2 appears.

Step 2 Select the desired policy and click **Delete**.

The Confirm Delete window appears

Step 3 Check the policy marked for deletion and click **OK**.

The Policies window refreshes and the selected policy disappears.

TE Tasks

Prime Fulfillment currently offers three TE-specific tasks that are used in a manner similar to other tasks:

- **TE Discovery (Full and Incremental)**—Populates the repository with data from the TE network. Discrepancies are reconciled and/or reported.
- **TE Functional Audit**—Performs functional audit on TE Primary or Backup SRs in certain states.
- **TE Interface Performance**—Calculates the interface/tunnel bandwidth utilization.

This section focuses on describing how to create TE Functional Audit and TE Interface Performance tasks. Instructions on how to create a TE Discovery task are included in Chapter 36, "TE Network Discovery".

Creating a TE Task

TE tasks are managed in the **Task Manager**, which is accessed by selecting **Operate > Task Manager**.

The Tasks window appears.

For a detailed description of the window elements in the Tasks window, see Chapter 52, "Task Manager".

This page shows all collection and deployment tasks that have been executed. Note that a task could be scheduled to happen once or there could be several scheduled runs of a task. The schedule can be viewed by selecting a task and clicking **Schedules**.

Creating a TE Functional Audit Task

For each tunnel in the SR, the TE Functional Audit task checks the LSP currently used on a router against the LSP stored in the repository:

- tunnel down—Ignore (do not check)
- tunnel up—Check the LSP used on the router against the one stored in the repository:
  - If they are the same, the tunnel and the SR are both set to **Functional**.
  - If they are different, both the tunnel and the SR are set to **Broken**.
- tunnel missing from router—SR left untouched. The tunnel state is set to **Lost**.

This task only performs functional audit on TE Primary or Backup SRs, which are not in one of the following states:

- **Closed**
- **Requested**
- **Invalid**
- **Failed Deploy**

For more information on working with service requests, see the managing service requests part elsewhere in this guide.

To create a TE Functional Audit task, use the following steps:

Step 1 Choose **Operate > Task Manager**.

Step 2 Click **Audit > TE Functional Audit** to open the Create Task window.

For a detailed description of the window elements in the Create Task window, see Chapter 52, "Task Manager".

Step 3 Modify the **Name** or **Description** fields as desired and click **Next**.

The Task Service Requests window appears.

Step 4 Click **Add** to add a task service request.

The Select Service Request(s) window appears.

Step 5 Select an SR using the **Select** button.

Note Only SRs of type TE Tunnel or TE Protection will be accepted.

The Selected Service Request(s) window closes and the selected task(s) now appears in the Task Service Requests window. To add other SRs, repeat the procedure in Step 4 and Step 5.

Step 6 In the Task Service Requests window, click **Next**.

The Task Schedules window appears.

Step 7 Click **Now** to start the task immediately or **Create** to create a task schedule.

When selecting **Now**, a line is added to the **Task Schedules** window. When selecting **Create**, the Task Schedule window appears.

Step 8 In the Task Schedule window, indicate when and how often to run the task.

Step 9 Click **OK**.

The scheduled task should now appear in the **Task Schedules** table.

Note The default setting is to schedule a single TE Functional Audit task to take place immediately ("**Now**").

Step 10 Click **Next**.

The Task Schedule window now shows the new task in its list of created tasks. A summary of the scheduled task appears.

Step 11 Click **Finish**.

This adds the task to the list of created tasks in the Tasks window.

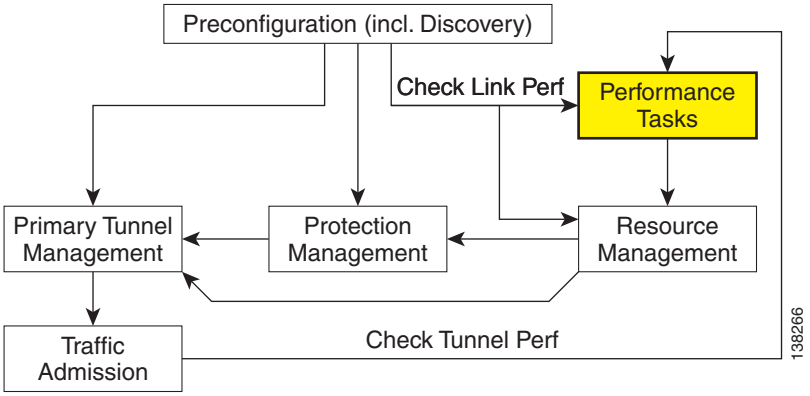
To view the task logs for the created tasks, see Viewing a Task Log, page 56-2.

Creating a TE Interface Performance Task

This task calculates interface/tunnel bandwidth utilization using the Simple Network Management Protocol (SNMP).

The highlighted box in Figure 42-3 shows where in Prime Fulfillment traffic admission occurs.

Figure 42-3 Prime Fulfillment Process Diagram - TE Interface Performance



Calculating utilization depends on how data is presented for the object you want to measure. Interface utilization is the primary measure used for network utilization. Because MIB-II variables are stored as counters, you must take two poll cycles and figure the difference between the two (hence, the delta used in the equation).

Three variables are required:

- task duration—how long the task will run (in seconds)
- frequency—how frequent the data will be collected (in seconds)
- interval—the distance between two poll cycles (in milliseconds).

The following explains the variables used in the formulas:

- delta(traffic in)—the delta between two poll cycles of collecting the SNMP input object, which represents the number of inbound units of traffic
- delta(traffic out)—the delta between two poll cycles of collecting the SNMP output object, which represents the number of outbound units of traffic
- bandwidth—the speed of the interface.

A more accurate method is to measure the input utilization and output utilization separately, using the following formula:

$$\text{Input utilization} = \frac{\text{delta(traffic in)} \times 8 \times 100}{\text{(number of seconds in delta)} \times \text{bandwidth}}$$

$$\text{Output utilization} = \frac{\text{delta(traffic out)} \times 8 \times 100}{\text{(number of seconds in delta)} \times \text{bandwidth}}$$

To create a TE Interface Performance task, use the following steps:

Step 1 Choose **Operate > Task Manager**.

Step 2 Click **Create > TE Interface Performance** to open the Create Task window for a new TE Interface Performance task.

For a detailed description of the window elements in the Create Task window, see Chapter 52, "Task Manager".

Step 3 Modify name and description if needed and click **Next**.

The Select TE Provider window appears.

Step 4 Click a radio button to select a TE provider.

Step 5 Click **Next**.

The TE Performance Collection window appears.

Step 6 Enter desired values in the **Task Duration**, **Task Frequency**, and **Task Interval** fields.

Note If the **Task Interval** field is set too low, the MIB might not be updated, in which case the TE Performance Report will not show any traffic. For tunnels or links on IOS routers, it is recommended to set the interval to 1000 ms; for IOS XR routers, a recommended interval is 5000 ms. Note that these values might need to be tuned to suit your specific environment.

Step 7 Use the **Add** button to select a tunnel or link on which to run the interface performance task:

- **TE Tunnel**—Add a TE tunnel. The Select Tunnel(s) window appears.
- **TE Link**—Add a TE link. The Select Link(s) window appears.

Step 8 Select one or more of tunnels and links and click **Next**.

The selected tunnels and links are added to the **Targets** list in the TE Performance Collection window. The Task Schedules window appears.

Step 9 Click **Now** or **Create** to create a task schedule.

When you select **Create** to customize the schedule, the Task Schedule window appears (with **Now**, this step is skipped).

Note The default setting is to schedule a single TE Interface Performance task to take place immediately ("**Now**").

Step 10 In the Task Schedule window, make your selections to define when and how often to run the task.

Step 11 Click **OK**.

The scheduled task should now appear in the **Task Schedules** table.

Step 12 Click **Next**.

A summary of the scheduled task appears.

Step 13 Click **Finish**.

This adds the task to the list of created tasks in the Tasks window.

To view the TE Performance Report that is generated for TE Interface Performance task(s), see TE Performance Reports, page 56-3.

To view the task logs for the created tasks, see Viewing a Task Log, page 56-2.

SR History and Configlets

The history and configlets associated with individual service requests can be viewed from the Service Requests window when you select a service request and click the **Details** button.

The history of a service request is essentially a state change report. It lists the various states that elements associated with an SR has transitioned between and reports relevant details pertaining to these state changes.

Configlets for devices associated with service requests are in simple scrollable text format.

For more information about these features and how to manage service requests, see the managing service requests part elsewhere in this guide.

Managing the Locking Mechanism

Whenever a task is performed that incurs a database update, which might affect the resource and hence the result of a tunnel computation, it locks the system before the update and releases it at completion of the update. If for some reason the lock is not released, other updates that require the lock are blocked.

The purpose of the lock feature is to prevent concurrent and mutually inconsistent planning activities from being committed to the database. Meaning, if each user takes the same snapshot of the the repository, performs computations, and tries to commit what he/she sees, the locking mechanism helps synchronize the commit and ensures that no commit invalidates other commits.

If the system is locked for prolonged periods of time, the administrator should check if anyone is performing long planning tasks and take note of which process locked the system and report it. If the administrator is sure that no one is using the system, it can be unlocked by using the lock manager.

Prime Fulfillment has two kinds of locks:

- TE provider lock—Locks managed tunnels, backup tunnels, resource SRs, and TE Discovery.
- TE router lock—Locks unmanaged tunnels.

Each system lock is linked to a TE provider. In the following, procedures for unlocking each system lock are listed.

Unlocking the TE Provider Lock

To unlock the TE provider, use the following steps:

Step 1 Choose **Traffic Engineering > Providers**.

The TE Providers window appears.

Step 2 Select a TE provider that is locked by checking the corresponding check box.

Step 3 Click **Manage Lock**.

The System Lock Management window appears.

The text fields in this window are read-only.

Step 4 To unlock, click the **Unlock** button.

The System Lock Management window closes and the **System Lock Status** field in the TE Providers window is updated accordingly.

Unlocking the TE Router Lock

To unlock the TE router lock, use the following steps:

Step 1 Choose **Traffic Engineering > Nodes**.

The TE Nodes List window appears.

Step 2 Select a TE node that is locked by clicking the corresponding check box.

Step 3 Click **Manage Lock**.

The System Lock Management window appears. The text fields in this window are read-only.

Step 4 To unlock, click the **Unlock** button.

The System Lock Management window closes and the **System Lock Status** field in the TE Nodes List window is updated accordingly.

Locking Operation Errors

TEM locks the TE Provider or TE Router object respectively for the duration of a save and deploy operation to ensure database consistency.

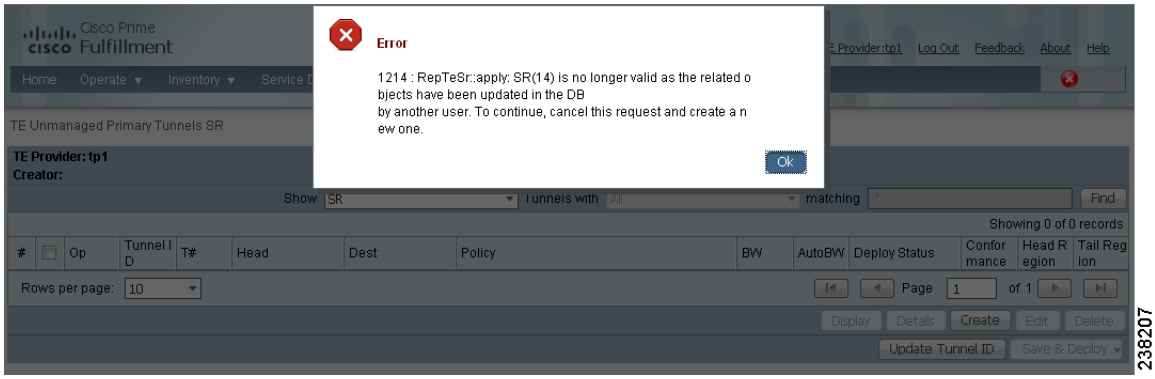
This section describes the following errors:

- Modifying Locked Object, page 42-11
- Modifying Object After Lock Is Released, page 42-12
- Deleting Link with Associated TE Object, page 42-12
- Deleting Link Without Associated TE Object, page 42-13

Modifying Locked Object

If you attempt to modify a locked object, you will be informed that the object cannot be modified because another user is making changes. You will receive the error message shown in Figure 42-4.

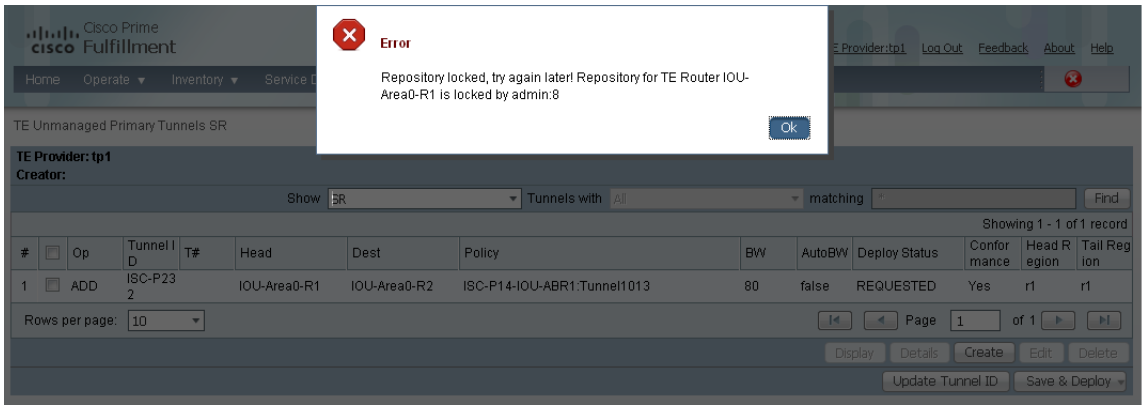
Figure 42-4 Modifying Locked Object



Modifying Object After Lock Is Released

If you attempt to modify an object after the lock is released, Prime Fulfillment will check that your current working version of the object is up to date. If not, you will be instructed to restart with a new version of the object as your data is now out of date. You will receive the error message shown in Figure 42-5.

Figure 42-5 Modifying Object After Lock Is Released

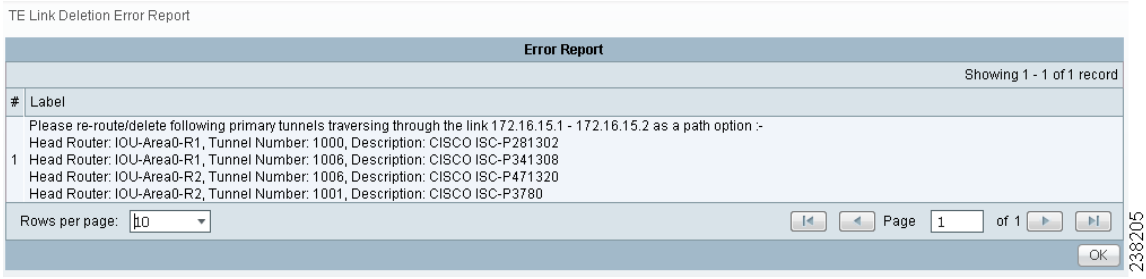


Deleting Link with Associated TE Object

Link removal is not allowed if the link is associated with an explicit path or is traversed by a tunnel.

If you try to delete a link with one or more associated objects, the error message in Figure 42-6 is displayed.

Figure 42-6 Deleting Link with Associated TE Object



Deleting Link Without Associated TE Object

A link can be removed if it is not traversed by a tunnel, even if it is associated with an explicit path. When you try to delete such a link, the type of report shown in Figure 42-7 will be displayed.

Figure 42-7 Deleting Link Without Associated TE Object