



CHAPTER 9

Deploying, Monitoring, and Auditing Service Requests

This chapter describes how to deploy, monitor and audit L2VPN, VPLS or FlexUNI/EVC service requests, and how to access task logs. It contains the following sections:

- [Deploying Service Requests, page 9-1](#)
- [Monitoring Service Requests, page 9-10](#)
- [Auditing Service Requests, page 9-12](#)

Deploying Service Requests

To apply L2VPN, VPLS, or FlexUNI policies to network devices, you must deploy the service request. When you deploy a service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet.

Pre-Deployment Changes

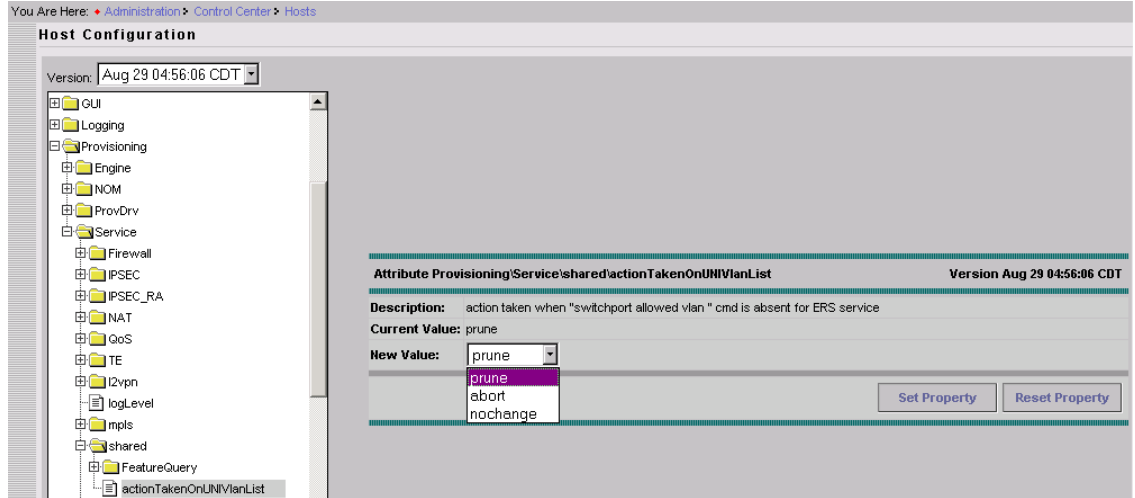
You can change the Dynamic Component Properties Library (DCPL) parameter **actionTakenOnUNIVlanList** before you deploy an L2VPN or VPLS service request. This will be necessary if the **trunk allowed vlan** list is not present on the User Network Interface (UNI).

To make this change, perform the following steps.

-
- Step 1** Choose **Administration > Control Center**.
 - Step 2** Choose the host that you want to change.
 - Step 3** Click **Config**.
 - Step 4** Choose **Provisioning > Service > shared > actionTakenOnUNIVlanList**.

The window shown in [Figure 9-1](#) appears.

Figure 9-1 Change DCPL Parameter



Step 5 Choose one of the following:

- **prune** to have ISC create the minimum VLAN list. This is the default.
- **abort** to have ISC stop the L2VPN or VPLS service request provisioning with the error message: **trunk allowed vlan list is absent on ERS UNI.**
- **nochange** to have ISC allow all VLANs.

Step 6 Click **Set Property**.

Service Deployment

After you create a service request and save it in the ISC repository, you can deploy or force-deploy it. Perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests window appears.

Step 2 Choose a service request.

Step 3 Click **Deploy** and choose **Deploy** or **Force-Deploy**.

Use **Deploy** when the service request state is Requested or Invalid.

Use **Force Deploy** when the service request state is Deployed, Failed Deployed, or Failed Audit.

The Deploy Service Requests window appears. (See [Figure 9-2](#).)

Figure 9-2 Schedule Service Activation

Deploy Service Requests

Task Name *:

Task Type :

Task Description :

Single run: Now Once

Periodic Run: Minute Hourly Daily Weekly Monthly

Periodic Run Attributes

Run Interval:

Run Limits:

Start Date and Time

Date:

Time:

End Date and Time (Default is unlimited)

Date:

Time:

Service Requests

Showing 1 - 1 of 1 record

#	Job ID	Creator	Customer Name	Description
1.	7	admin	Customer1	

Rows per page: Go to page: of 1

Note: * - Required Field

138606

Step 4 Choose a schedule for the activation of the service.

Step 5 After you schedule the service request, click **Save**.

After you schedule the service request, you can monitor the service request that is being deployed. See [Verifying Service Requests, page 9-3](#) and [Monitoring Service Requests, page 9-10](#) for more information.

Verifying Service Requests

After you deploy a service request, you should verify that there were no errors.

You can verify a service request through the following:

- Transition state—The transition state of a service request is listed on the Service Requests window in the State column. When the service request is successfully deployed, its state changes to DEPLOYED. For more information, see [Service Request States, page 9-4](#).

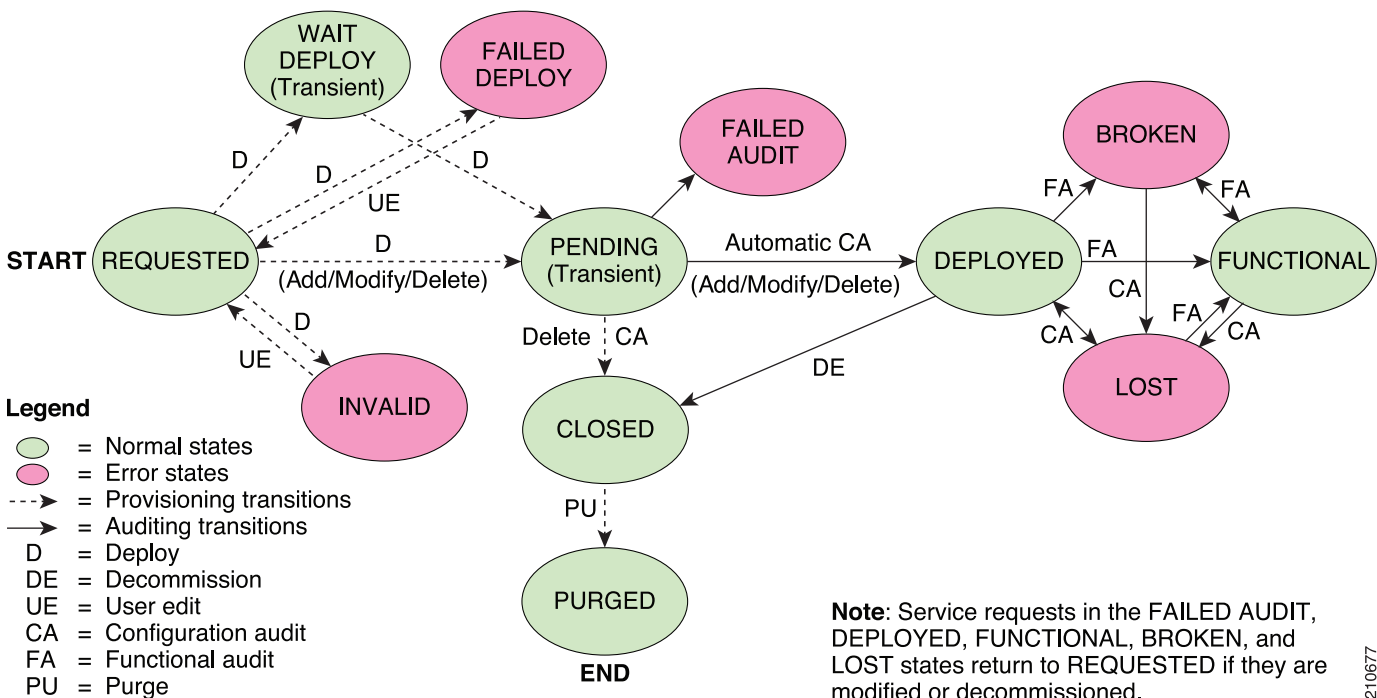
- View service request details—From the Service Requests Details window, you can view the link endpoints and the configlets for this service request. For more information, See [Viewing Service Request Details, page 9-7](#).
- Task Logs—Access the task logs from the Monitoring tab to help you troubleshoot a failed service request or to view more details about a service request. For more information, see [Monitoring Service Requests, page 9-10](#).

Service Request States

A service request transition state describes the different stages a service request enters during the provisioning process. For example, when you deploy a service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet. When the configlet is generated and downloaded to the device, the service request enters the **Pending** state. When the device is audited, the service request enters the **Deployed** state.

Figure 9-3, “Service Requests States Transition Diagram,” shows a high-level diagram of the relationships and movement among ISC service request states.

Figure 9-3 Service Requests States Transition Diagram



210677

Table 9-1, “Summary of Cisco IP Solution Center Service Request States,” describes the functions of each ISC service request state. They are listed in alphabetic order.

Table 9-1 Summary of Cisco IP Solution Center Service Request States

Service Request Type	Description
Broken (valid only for MPLS services)	The router is correctly configured but the service is unavailable (due to a broken cable or Layer 2 problem, for example). An MPLS service request moves to Broken if the auditor finds the routing and forwarding tables for this service, but they do not match the service intent.
Closed	A service request moves to Closed if the service request should no longer be used during the provisioning or auditing process. A service request moves to the Closed state only upon successful audit of a decommission service request. ISC does not remove a service request from the database to allow for extended auditing. Only a specific administrator purge action results in service requests being removed.
Deployed	A service request moves to Deployed if the intention of the service request is found in the router configuration file. Deployed indicates that the configuration file has been downloaded to the router, and the intent of the request has been verified at the configuration level. That is, ISC downloaded the configlets to the routers and the service request passed the audit process.
Failed Audit	This state indicates that ISC downloaded the configlet to the router successfully, but the service request did not pass the audit. Therefore, the service did not move to the Deployed state. The Failed Audit state is initiated from the Pending state. After a service request is deployed successfully, it cannot re-enter the Failed Audit state (except if the service request is redeployed).
Failed Deploy	The cause for a Failed Deploy status is that DCS reports that either the upload of the initial configuration file from the routers failed or the download of the configuration update to the routers failed (due to lost connection, faulty password, and so on).
Functional (valid only for MPLS services)	An MPLS service request moves to Functional when the auditor finds the VPN routing and forwarding tables (VRF) for this service and they match with the service intent. This state requires that both the configuration file audit and the routing audit are successful.
Invalid	Invalid indicates that the service request information is incorrect in some way. A service request moves to Invalid if the request was either internally inconsistent or not consistent with the rest of the existing network/router configurations (for example, no more interfaces were available on the router). The Provisioning Driver cannot generate configuration updates to service this request.
Lost	A service request moves to Lost when the Auditor cannot find a configuration-level verification of intent in the router configuration files. The service request was in the Deployed state, but now some or all router configuration information is missing. A service request can move to the Lost state <i>only</i> when the service request had been Deployed .

Table 9-1 Summary of Cisco IP Solution Center Service Request States (continued)

Service Request Type	Description
Pending	<p>A service request moves to Pending when the Provisioning Driver determines that the request looks consistent and was able to generate the required configuration updates for this request. Pending indicates that the service request has generated the configuration updates and the configuration updates are successfully downloaded to the routers.</p> <p>The Auditor regards pending service requests as new requests and begins the audit. If the service has been freshly provisioned and not yet audited, it is not an error (pending audit). However, if an audit is performed and the service is still pending, it is in an error state.</p>
Requested	<p>If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains Requested, the service is in an error state.</p>
Wait Deploy	<p>This service request state pertains only when downloading configlets to a Cisco CNS-CE server, such as a Cisco CNS IE2100 appliance. Wait Deploy indicates that the configlet has been generated, but it has not been downloaded to the Cisco CNS-CE server because the device is not currently online. The configlet is staged in the repository until such time as the Cisco CNS-CE server notifies ISC that it is up. Configlets in the Wait Deploy state are then downloaded to the Cisco CNS-CE server.</p>

Table 9-2, “User Operations on ISC Service Requests,” describes user operations and their impact on ISC service requests.

Table 9-2 User Operations on ISC Service Requests

User Operations	Description
Decommission	<p>This user operation removes the service from all devices in the service request.</p>
Force Deploy	<p>This user operation allows you to Deploy a service request from any state except Closed. This is equivalent to restarting the state diagram. The service request can move from its current state to any other possible state. However, it does not move to the Requested state.</p>
Force Purge	<p>This user operation removes a service request from the database irrespective of its state. If you Force Purge a service request from the ISC repository before first decommissioning the service request, the service remains running on the network (specifically, the configuration remains on the devices on which the service was provisioned), but all record of the service request that created the service is removed from ISC.</p>
Purged	<p>When a service request is Purged, it is removed from the ISC database.</p>

Viewing Service Request Details

The service request details include the link endpoints for the service request, the history, and the configlet generated during the service request deployment operation. Use the service request details to help you troubleshoot a problem or error with the service request or to check the commands in the configlet.

From the Service Request Details page, you can view more information about:

- Links—the link endpoint details
- History—Service request history report
- Audit—Audit reports for the link IDs
- Configlets—View the ISC generated configlet for the L2VPN or VPLS service request

The following sections describe the links, history, and configlet details for an L2VPN or VPLS service request. The audit details are described in [Auditing Service Requests, page 9-12](#).

To view service request details, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.
The Service Requests window appears.
- Step 2** Choose the service request and click **Details**.
The Service Request Details window appears. (See [Figure 9-4](#).)

Figure 9-4 Example Service Request Details Window

Attribute	Value
Type	L2VPN
State	REQUESTED
Operation Type	MODIFY
Service Request ID	5
Last Modification Time	Wed Nov 23 15:21:29 PST 2005
L2VPN Service Type	L2VPN_EBS
L2VPN Core Type	MPLS
EndToEndWire ID 5	
Status Message	
State	REQUESTED
VC ID	100
Attachment Circuit ID 7	
N-PE Name	pe1
N-PE Interface	Ethernet4/3.20
CE Name	ce3
CE Interface	Ethernet0/1.20
VLAN ID	20
Attachment Circuit ID 8	

The service request attribute details include the type, transition state, operation type, ID, modification history, customer, and policy name.

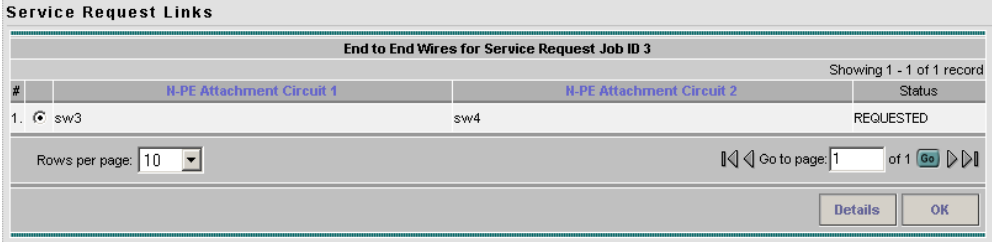
Links

The service request link details include the link endpoints, PE secured interface, VLAN ID, and whether a CE is present.

To see this information, perform the following steps.

- Step 1** Click **Links** on the Service Request Details window. (See [Figure 9-4](#).)
The Service Request Links window appears. (See [Figure 9-5](#).)

Figure 9-5 Service Request Links



Service Request Links			
End to End Wires for Service Request Job ID 3			
#	N-PE Attachment Circuit 1	N-PE Attachment Circuit 2	Status
1.	sw3	sw4	REQUESTED

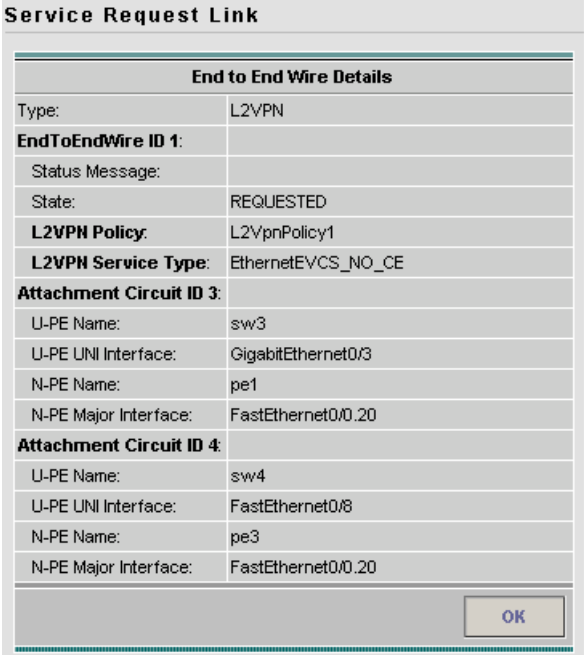
Showing 1 - 1 of 1 record

Rows per page: 10 of 1 of 1 Go

Details OK

- Step 2** Choose a link and click **Details**.
The Link Details window appears. (See [Figure 9-6](#).)

Figure 9-6 Link Details Window



Service Request Link	
End to End Wire Details	
Type:	L2VPN
EndToEndWire ID 1:	
Status Message:	
State:	REQUESTED
L2VPN Policy:	L2VpnPolicy1
L2VPN Service Type:	EthernetEVCS_NO_CE
Attachment Circuit ID 3:	
U-PE Name:	sw3
U-PE UNI Interface:	GigabitEthernet0/3
N-PE Name:	pe1
N-PE Major Interface:	FastEthernet0/0.20
Attachment Circuit ID 4:	
U-PE Name:	sw4
U-PE UNI Interface:	FastEthernet0/8
N-PE Name:	pe3
N-PE Major Interface:	FastEthernet0/0.20

OK

- Step 3** Click **OK** to return to the Service Request Links window.
Step 4 Choose another link to view or click **OK** to return to the Service Request Details window.

History

To view history information about the service request, perform the following steps.

- Step 1** Click **History** on the Service Request Details window. (See [Figure 9-4](#).)
The Service Request State Change Report window appears. (See [Figure 9-7](#).)

Figure 9-7 Service Request State Change Report

Service Request State Change Report			
Element Name	State	Create Time	Report
L2VPN Service Request	PENDING	2005-09-15 14:15:03	SR Job ID 13 transitioned from REQUESTED to PENDING state
L2VPN Service Request	DEPLOYED	2005-09-15 14:15:23	SR Job ID 13 transitioned from PENDING to DEPLOYED state

OK

The history reports lists the following information about the service request:

- Element Name—the device, interface, and subinterfaces participating in this service request
- State—the transition states the element has gone through
- Create Time—the time the element was created for this service request
- Report—the action taken by ISC for the element in this service request

- Step 2** Click **OK** to return to the Service Request Details window.

Configlets

After you deploy the service request, ISC generates Cisco IOS commands to turn on L2VPN or VPLS Services on all the network devices that participate in the service request.

To view the configlets that are generated, perform the following steps.

- Step 1** Click **Configlets** on the Service Request Details window. (See [Figure 9-4](#).)
You see a list of network devices for which a configlet was generated. (See [Figure 9-8](#).)

Figure 9-8 Service Request Configlets

Service Request Configlets	
Configlets for Service Request Job ID 13	
Showing 1 - 4 of 4 records	
#	Device
1.	ce3
2.	ce8
3.	pe1
4.	pe3

Rows per page: 10 Go to page: 1 of 1

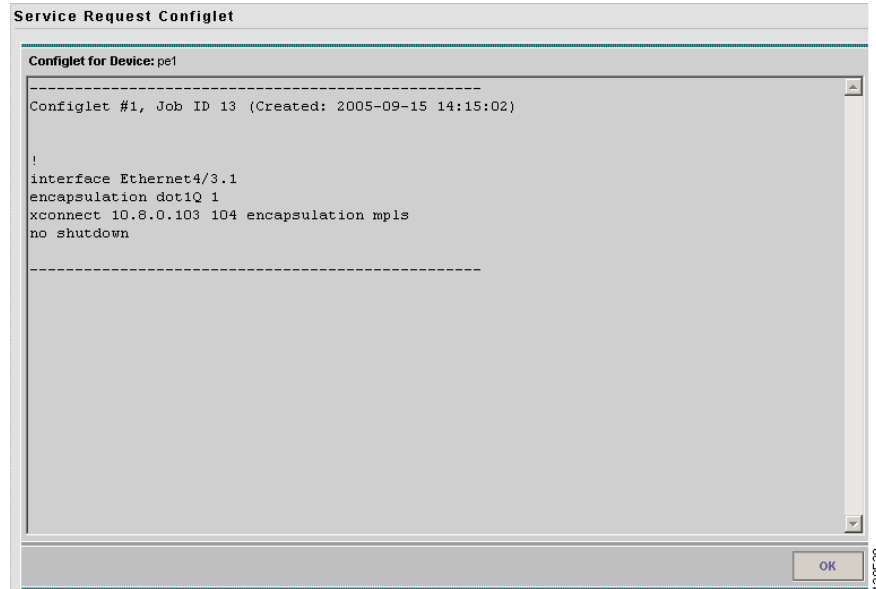
View Configlet OK

- Step 2** Choose the device for which you want to view the configlet.

Step 3 Click **View Configlet**.

The Configlet for Device window appears. (See [Figure 9-9](#).)

Figure 9-9 L2VPN or VPLS Configlet Example



The device configlet shows all commands downloaded to the device configuration during the service request deployment operation.

Step 4 Click **OK** to exit.

Monitoring Service Requests

To monitor a service request that is being deployed, you must use the task logs to help you troubleshoot why a service request has failed or to find more details about a service request.

To monitor a service request, perform the following steps.

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

The Tasks window appears. (See [Figure 9-10](#).)

Figure 9-10 Tasks Window

#	Task Name	Type	Targets	Schedule	Creator	Created on
1	Task Created 2005-09-15 15:01:23.977	Service Deployment	Job Id : 18 Vpn : I2vpn_ers_vpn3	Single run at 2005-09-15 15:00:00.0	admin	2005-09-15 15:01:28.782
2	Task Created 2005-09-15 14:50:58.069	Service Deployment	Job Id : 17 Vpn : I2vpn_ers_vpn	Single run at 2005-09-15 14:50:00.0	admin	2005-09-15 14:51:08.508
3	Task Created 2005-09-15 14:21:02.448	Service Deployment	Job Id : 3 Vpn : Vpn1 Job Id : 4 Vpn : Job Id : 5 Vpn : Vpn2 Job Id : 6 Vpn : Vpn3 Job Id : 7 Vpn : Vpn4	Single run at 2005-09-15 14:21:00.0	admin	2005-09-15 14:21:07.05
4	Task Created 2005-09-15 14:13:33.063	Service Deployment	Job Id : 13 Vpn : I2vpn_ers_vpn	Single run at 2005-09-15 14:13:00.0	admin	2005-09-15 14:13:41.907

Step 2 Click **Find** to refresh the window.

The task that is executing will be the first in the list of tasks that being performed in ISC.

Step 3 Choose the task you want to monitor and click **Logs**.

The Task Logs window appears. (See [Figure 9-11](#).)

Figure 9-11 Task Logs

#	Runtime Task Name	Action	Start Time	End Time	Status
1	Task Created 2005-09-15 15:01:23.977_Thu_Sep_15_15:01:32_PDT_2005_3	ConfigAudit	2005-09-15 15:02:11.229	2005-09-15 15:02:49.739	Completed successfully
2	Task Created 2005-09-15 15:01:23.977_Thu_Sep_15_15:01:32_PDT_2005_3	Deployment	2005-09-15 15:01:33.534	2005-09-15 15:02:11.201	Completed successfully

Step 4 Choose the run-time task that you want to monitor and click **View Log**.

A window like the one shown in [Figure 9-12](#) appears.

Figure 9-12 Task Logs

Date	Level	Component	Message
2005-09-15 15:02:11	INFO	Provisioning.ProvDrv	The argument to the ProvDrv are: isProvision = false JITUpload = false JobIdList = 18 targets = []
2005-09-15 15:02:11	INFO	Provisioning.ProvDrv	Opening repository ...
2005-09-15 15:02:11	INFO	Provisioning.ProvDrv	Open repository succeeded
2005-09-15 15:02:11	INFO	Provisioning.ProvDrv	===== Creating ProvDrvSR for Job#18SR#18
2005-09-15 15:02:11	INFO	Provisioning.ProvDrv	Filter to getLogicalDevices: 0
2005-09-15 15:02:11	INFO	GSAM	getServiceElements() : ACTION -> AUDIT
2005-09-15 15:02:11	INFO	Provisioning.ProvDrv	Number of logicalDevices got: 3
2005-09-15 15:02:12	INFO	Provisioning.ProvDrv	Processing logical device 3 with physical id 3
2005-09-15 15:02:12	INFO	Provisioning.ProvDrv	Service blade for this device: com.cisco.vpnsc.prov.l2vpn.L2VPNServiceBlade
2005-09-15 15:02:12	INFO	Provisioning.ProvDrv	Create blade the first time: com.cisco.vpnsc.prov.l2vpn.L2VPNServiceBlade
2005-09-15 15:02:12	INFO	Provisioning.Service.l2vpn	created service blade
2005-09-15 15:02:12	INFO	Provisioning.Service.l2vpn	returning XML_JDOM as preference
2005-09-15 15:02:12	INFO	Provisioning.ProvDrv	Filter to generateXML: 0

- Step 5** Choose the log level from the drop-down list and click **Filter**.
The log levels are All, Severe, Warning, Info, Config, Fine, Finer, and Finest.
- Step 6** Click **Return to Logs**.
- Step 7** Click **Close** in the Task Logs window.

Auditing Service Requests

Each time a service request is deployed in the Cisco IP Solution Center (ISC), a configuration audit occurs. You can view the results of these in configuration audit reports. Use configuration audits and reports to verify that the network devices have the correct configuration for the services provided.

A configuration audit occurs automatically each time you deploy a service request. During this configuration audit, ISC verifies that all Cisco IOS commands are present and that they have the correct syntax. An audit also verifies that there were no errors during deployment.

The configuration audit verifies the service request deployment by examining the commands configured by the service request on the target devices. If the device configuration does not match what is defined in the service request, the audit flags a warning and sets the service request to a **Failed Audit** or **Lost** state.

You can create audit reports for new or existing service requests.

- Audit new services—This type of audit is for service requests that have just been deployed. The audit identifies problems with the configuration files downloaded to the devices.
- Audit existing services—This type of audit checks and evaluates the configuration of deployed service requests to see if the service request is still in effect.

We recommend that you schedule a service request audit on a regular basis to verify the state of the network provisioning requests.

This section describes how to manually generate a configuration audit and view the audit report.

To view a configuration audit report, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.
The Service Requests window appears.
- Step 2** Choose an service request for the configuration audit.
- Step 3** Click **Details**.
The Service Request Details window appears.
- Step 4** Click **Audit**.
- Step 5** Click **Config**.
The Service Request Audit window appears. [Figure 9-13](#) shows an example of a successful configuration audit.

Figure 9-13 Service Request Audit Report—Successful

Service Request Audit Report				
Config Audit Report for Job ID 13				
Service Request ID: 13			Status: SUCCESSFUL	
Link ID	Status	Device Name	Device Role	Device Messages
8	SUCCESSFUL	ce8	CE	
		pe3	N_PE	
		ce3	CE	
		pe1	N_PE	

This window lists the device name and role, and a message regarding the status of your configuration audit.

If the audit is unsuccessful, the message field lists details on the failed audit. [Figure 9-14](#) shows an example of a failed audit message for an service request.

Figure 9-14 Service Request Audit Report—Failed

Service Request Audit Report				
Config Audit Report for Job ID 13				
Service Request ID: 13			Status: FAILED	
Link ID	Status	Device Name	Device Role	Device Messages
8	FAILED	ce8	CE	
		pe3	N_PE	layer 2 Ether failed (command: interface Ethernet1/1.1) EC ether failed (command: interface Ethernet1/1.1) PE loopback specified in the PE device table doesn't exist on the router (command: NO CONFIG INVOLVED)
		ce3	CE	
		pe1	N_PE	layer 2 Ether failed (command: interface Ethernet4/3.1) EC ether failed (command: interface Ethernet4/3.1) PE loopback specified in the PE device table doesn't exist on the router (command: NO CONFIG INVOLVED)

The audit failure message indicates missing commands and configuration issues. Carefully review the information in the message field. If the audit fails, you must correct all errors and redeploy the service request.

- Step 6** Click **OK** to return to the Service Request Details window.

