



Provisioning Services

In ISC you provision services through service requests. This chapter explains how to deploy, change, audit, and decommission service requests. This chapter contains the following sections:

- [Deploying Service Requests, page 7-1](#)
- [Viewing the Service Request State, page 7-3](#)
- [Modifying Service Requests, page 7-6](#)
- [Viewing Service Request Details, page 7-6](#)
- [Auditing Service Requests, page 7-9](#)
- [Viewing Task Logs, page 7-18](#)
- [Decommissioning a Service Request, page 7-18](#)



Note

Before creating an ISC security policy or service request, it is necessary to populate the ISC repository with the target devices in your network, collect the initial device configuration files, designate customers and customer sites, and define each target device as a CPE device.

CPE devices are the devices at each end of the VPN tunnel. Creating CPE devices includes assigning each target device to a specific customer and customer site and marking the device interfaces. Specifically for security management, you define at least one public (outside) and one private (inside) interface on each device.

For how-to information on populating your ISC repository and setting up CPE devices, refer to the *Cisco IP Solution Center Infrastructure Guide, 3.0*.

Deploying Service Requests

After a service request has been defined, you can deploy it. To deploy the service request, perform the following the steps:

- Step 1** Click **Service Inventory > Inventory and Connection Manager > Service Requests**. The Service Requests page appears.

Figure 7-1 The Service Request Page Populated with Service Requests

The screenshot displays the 'Service Requests' page in the Cisco IP Solution Center. The page is titled 'Service Requests' and shows a table of 9 service requests. The table has the following columns: #, Job ID, State, Type, Operation Type, Creator, Customer Name, Policy Name, Last Modified, and Description. The data rows are as follows:

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	1	REQUESTED	QoS	ADD	admin	Customer1	Customer1_QoS_Policy	4/8/03 2:06 PM	
2.	2	REQUESTED	MPLS	ADD	admin	Customer1	Customer1_MPLS_Po...	4/8/03 2:09 PM	
3.	3	FAILED_DEPLOY	L2VPN	ADD	admin	Customer1	Customer1_L2VPN_P...	6/10/03 4:50 PM	
4.	4	REQUESTED	Firewall	MODIFY	admin	Customer1	Perimeter Firewalls	6/13/03 4:00 PM	This is service request f
5.	5	PENDING	IPsec	ADD	admin	Customer2	Pure	6/17/03 1:16 PM	
6.	6	REQUESTED	IPsec RA	ADD	admin	Customer2	Group1	6/17/03 1:35 PM	
7.	7	REQUESTED	NAT	MODIFY	admin	Customer1		6/21/03 8:18 PM	NAT service request 1
8.	10	PENDING	MPLS	ADD	backendadm		Discovered_Provid...	6/20/03 10:33 AM	
9.	11	PENDING	MPLS	ADD	backendadm		Discovered_Provid...	6/20/03 10:33 AM	

The page also includes a search bar at the top with 'Show Services with Job ID matching * of type All' and a 'Find' button. A 'Deploy' dropdown menu is open over the table, showing 'Deploy' and 'Force Deploy' options. The page number '98146' is visible on the right side.

- Step 2 Check the box next to the service request you want to deploy.
- Step 3 Click **Deploy**.
- Step 4 Choose **Deploy** or **Force Deploy** from the **Deploy** drop-down list. Use **Deploy** for new service requests, and **Force Deploy** for service requests to which you have made modifications and want to redeploy. **Force Deploy** freshly downloads the latest configuration in the service request to all CPE devices in the service request, even if the service request is already in the Deployed state. Also, use **Force Deploy** when a device configuration is lost or when you replace or change equipment in a CPE device definition.
- Step 5 The Deploy Service Requests page appears.

Figure 7-2 The Deploy Service Requests Page

Service Inventory | **Service Design** | **Monitoring** | **Administration**

Inventory and Connection Manager > Deployment Flow Manager > Device Console

You Are Here: > Service Inventory > Inventory and Connection Manager > Service Requests

Deploy Service Requests

Task Name * : Task Created 2003-06-25 01:11:17.585

Task Type: Deployment

Task Description: Created on Wed Jun 25 01:11:17 PDT 2003

Single Run: Now Once

Periodic Run: Minute Hourly Daily Weekly Monthly

Periodic Run Attributes

Run Interval:

Run Limits:

Start Date and Time

Date: June 25 2003

Time: 1 11 AM

End Date and Time (Default is unlimited)

Date: Month Day Year

Time: Hour Min AM

Save Cancel

Note: * - Required Field

98147

Step 6 Choose when you would like the service request to deploy.

Step 7 If you want to deploy the service request now, accept the default value and click **Save**.

Viewing the Service Request State

The status of a service request is displayed in its state, which may be Requested, Pending, Closed, Wait Deploy, Deployed, Failed Audit, Failed Deploy, Invalid, Lost, Broken, or Functional, as described in [Table 7-1](#). For example, when you create a service request, it is in a REQUESTED state. Once you deploy the service request, the state moves to PENDING and, if successfully deployed, to DEPLOYED.

The possible relationships between the service request states are illustrated in [Figure 7-3](#). You can view the service request state on the Service Requests page in the **State** column. (Click **Service Inventory** > **Inventory and Connection Manager** > **Service Requests** to reach the Service Requests page.)

Figure 7-3 Service Request States

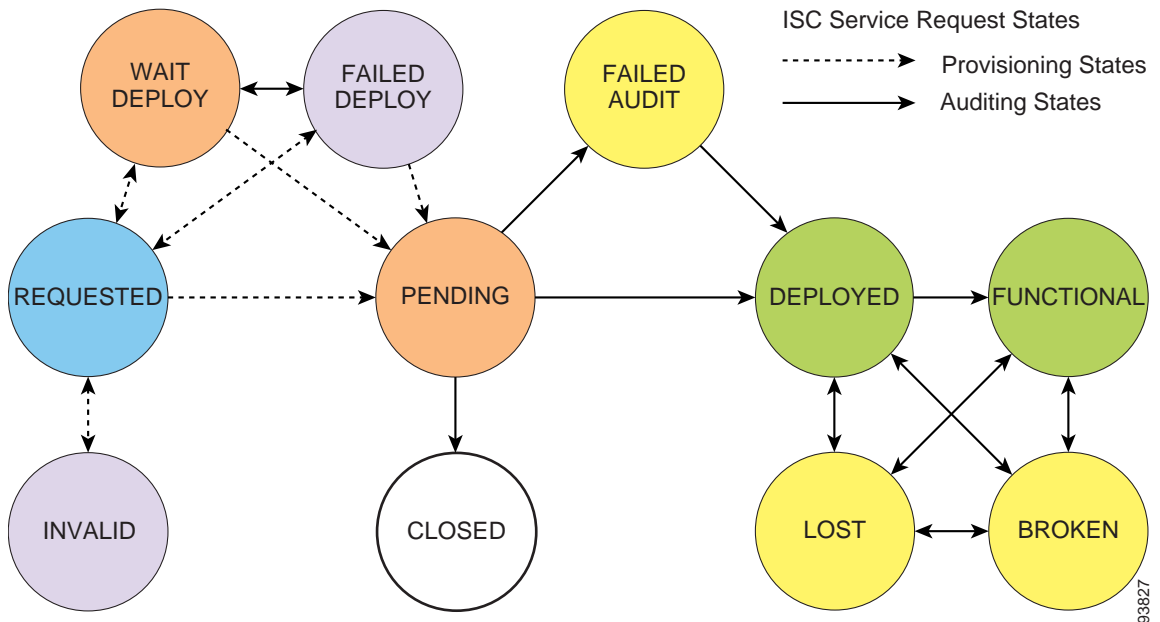


Table 7-1 Service Request States

Service Request Type	Description
Broken	<p>The router is correctly configured but the service is unavailable (due to a broken cable or Layer 2 problem, for example).</p> <p>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.</p> <p>An IPsec service request moves to Broken if a ping fails for all the remote peers of the current device.</p>
Closed	<p>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.</p>
Deployed	<p>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.</p>
Failed Audit	<p>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. Once a service request is deployed successfully, it cannot re-enter the Failed Audit state (except if the service request is redeployed).</p>

Table 7-1 Service Request States (continued)

Service Request Type	Description
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	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. An IPsec service request moves to Functional when the auditor finds that the router is configured properly and the IPsec traffic is flowing (ping is used to determine if IPsec traffic is flowing).
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 .
Pending	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. 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.
Requested	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.
Wait Deployed	This service request state pertains only when downloading configlets to a Cisco CNS-CE server, such as a Cisco CNS IE2100 appliance. Wait Deployed 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 Deployed state are then downloaded to the Cisco CNS-CE server.

Modifying Service Requests

To make configuration changes, you need to modify the service request and then redeploy it. To modify a service request, perform the following steps:

- Step 1** Click **Service Inventory > Inventory and Connection Manager > Service Requests** to reach the Service Requests page.
- Step 2** Check the box of the service request you want to modify and click **Edit**.
- Step 3** Make your changes and click **Save** to modify the service request, or click **Cancel** to exit without modifying the service request.
- Step 4** Clicking **Save** puts the service request into a REQUEST state and the **Operation Type** column changes to MODIFY as shown in [Figure 7-4](#).

Figure 7-4 Service Request MODIFY Operation Type

The screenshot shows the 'Service Requests' page in the Cisco IP Solution Center. The page has a navigation bar with tabs for 'Service Inventory', 'Service Design', 'Monitoring', and 'Administration'. Below the navigation bar, there are dropdown menus for 'Inventory and Connection Manager', 'Deployment Flow Manager', and 'Device Console'. The main content area is titled 'Service Requests' and contains a table of service requests. The table has the following columns: #, Job ID, State, Type, Operation Type, Creator, Customer Name, Policy Name, Last Modified, and Description. The table contains 9 rows of data. The 7th row is selected, and its 'Operation Type' is 'MODIFY'. The 'State' is 'REQUESTED'. The 'Description' is 'NAT service request 1'. Below the table, there are controls for 'Rows per page' (set to 10), 'Auto Refresh' (checked), and buttons for 'Create', 'Details', 'Edit', 'Deploy', 'Decommission', and 'Purge'.

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	1	REQUESTED	QoS	ADD	admin	Customer1	Customer1_QoS_Policy	4/8/03 2:06 PM	
2.	2	REQUESTED	MPLS	ADD	admin	Customer1	Customer1_MPLS_Po...	4/8/03 2:09 PM	
3.	3	FAILED_DEPLOY	L2VPN	ADD	admin	Customer1	Customer1_L2VPN_P...	6/10/03 4:50 PM	
4.	4	REQUESTED	Firewall	MODIFY	admin	Customer1	Perimeter Firewalls	6/13/03 4:00 PM	This is service request for
5.	5	PENDING	IPsec	ADD	admin	Customer2	Pure	6/17/03 1:16 PM	
6.	6	REQUESTED	IPsec RA	ADD	admin	Customer2	Group1	6/17/03 1:35 PM	
7.	7	REQUESTED	NAT	MODIFY	admin	Customer1		6/21/03 8:18 PM	NAT service request 1
8.	10	PENDING	MPLS	ADD	backendadm		Discovered_Provid...	6/20/03 10:33 AM	
9.	11	PENDING	MPLS	ADD	backendadm		Discovered_Provid...	6/20/03 10:33 AM	

- Step 5** Click **Deploy > Deploy** or **Force Deploy** to redeploy the service request. If you change the parameters of a policy or AAA server service request used in a deployed service request, then use **Force Deploy** to redeploy the modified service request.

Viewing Service Request Details

To view the details of a service request, perform the following steps:

- Step 1** Click **Service Inventory > Inventory and Connection Manager > Service Requests**.

- Step 2** Put a check mark next to the service request for which you want to view the details.
- Step 3** Click **Details**. The Service Request Details page appears. From the Service Request Details page, you can view the history of the service request, audit reports, and the configlets generated by the service request as well as the VPN tunnel details.

Figure 7-5 The Service Request Details Page

The screenshot displays the 'Service Request Details' page for Job ID 7. The page is part of the 'Inventory and Connection Manager' interface. A table lists various attributes and their corresponding values. At the bottom right of the table, there are four buttons: 'History', 'Audit', 'Configlets', and 'OK'. A vertical label '98148' is present on the right side of the screenshot.

Service Request Details for Job ID 7	
Attribute	Value
Type	NAT
State	REQUESTED
Operation Type	ADD
Service Request ID	12
Last Modification Time	Sat Jun 21 20:18:27 PDT 2003
Customer	Customer1
CPE Name	ence21
Site Name	Site-ence21
Operation Type	MODIFY
State	REQUESTED
Status Message	

- Step 4** Click **History** to view the history report. The Service Request History Report page appears. This page shows you the history of the service request state.

Figure 7-6 Service Request History Report

The screenshot shows the Service Inventory interface with the 'Service Request History Report' displayed. The breadcrumb path is: You Are Here: Service Inventory > Inventory and Connection Manager > Service Requests. The report table contains the following data:

Element Name	State	Create Time	Report
	REQUESTED	2003-06-21 20:18:27	SR Job ID 7 was subsumed: Old SR ID = 7, New SR ID = 12
	REQUESTED	2003-06-21 20:18:27	SR Job ID 7 remaining at REQUESTED state

An 'OK' button is visible at the bottom right of the report area.

98150

- Step 5** Click **OK** when done.
- Step 6** Click **Audit** to view service request audit information.
- Step 7** Click **Configlets** to view configlets generated by the service request. The Service Request Configlets page appears.

Figure 7-7 Service Request Configlets

The screenshot shows the 'Service Request Configlets' page for Service Request Job ID 3. It displays a table with 3 records:

#	Select	Device
1.	<input checked="" type="radio"/>	Device_3k1
2.	<input type="radio"/>	Device_R1
3.	<input type="radio"/>	Device-pix1

Below the table, there is a 'Rows per page' dropdown set to 10. At the bottom right, there are 'View Configlet' and 'OK' buttons.

98130

- Step 8** Choose the device for which you want to see the configlet and click **View Configlet**. The Configlet for Device page appears.

Figure 7-8 Configlet for Device

```

Service Request Configlet

Configlet for Device: Device_R1
-----
Configlet #1 (Created: 2003-04-14 15:53:57)
  Job #3      Service Request #3

aaa authentication login ISC_RA_USER_AAA group radius
aaa authorization network ISC_RA_GROUP_AAA local
radius-server host 192.168.116.12 timeout 4 retransmit 2 key secret
ip radius source-interface Ethernet0/0
crypto map ISC_CME client authentication list ISC_RA_USER_AAA
crypto map ISC_CME isakmp authorization list ISC_RA_GROUP_AAA
crypto map ISC_CME client configuration address respond
crypto isakmp client configuration group Policy1
  key password1
!
crypto isakmp keepalive 90 12
crypto isakmp policy 3330
  encr 3des
  hash md5
  group 2
  lifetime 86400
  authentication pre-share
!
crypto ipsec transform-set ISC_TS_1 esp-3des esp-md5-hmac
crypto dynamic-map ISC_CME 1
  set transform-set ISC_TS_1
  
```

Step 9 Click **OK** to exit.

Auditing Service Requests

From time to time, you may want to run audit tasks to check if the configurations on the devices in your network match the configlets generated by a deployed service request. In ISC, you can run an audit task to do this. The auditing features in ISC are located under **Home > Monitoring > Task Manager > Tasks**. Additionally, you can set audit tasks to run once or at a later time, or schedule them to run periodically. For more details on how to run audit tasks in general, refer to the *Cisco IP Solution Center: Infrastructure Reference, 3.0*.

To view an audit report, go to the [“Viewing Service Request Details”](#) section on page 7-6.

Config Audit

When you deploy a service request, ISC checks the configlet that it deployed against the configuration on the CPE device (this is called a **Config Audit**). If both configlets are the same, the audit is successful.

To manually run a **Config Audit**, click **Home > Monitoring > Task Manager > Tasks** and refer to the *Cisco IP Solution Center: Infrastructure Reference, 3.0* for instructions on how to start Task Manager and create a **Config Audit** task.

Certificate Enrollment Audit

Certificate enrollment audits can be performed for site-to-site and remote access service requests only.

- Step 1** To run a certificate enrollment audit, click **Home > Monitoring > Task Manager > Tasks**. The Tasks page appears as shown in [Figure 7-16](#).

Figure 7-9 The Tasks Page

The screenshot shows the 'Tasks' page in the Cisco Service Inventory Monitoring interface. The breadcrumb path is 'You Are Here: Monitoring > Task Manager > Tasks'. The page title is 'Tasks'. There is a search bar with the text 'Show Tasks with Task Name matching *' and 'of type *'. Below the search bar, it says 'Showing 1-3 of 3 records'. The table has the following data:

#	Task Name	Type	Schedule	Creator
1.	c1	Collect Config	Single run at 2003-04-08 13:42:00.0	admin
2.	Deployment Flow Task 2003-04-08 14:40:27.644	Deployment Flow	Single run at 2003-04-08 14:40:00.0	admin
3.	Task Created 2003-06-10 16:44:15.292	Service Deployment	Single run at 2003-06-10 16:44:00.0	admin

Below the table, there is a 'Rows per page:' dropdown set to '10'. There is an 'Auto Refresh:' checkbox which is checked. At the bottom right, there are buttons for 'Create', 'Details', 'Schedules', and 'Delete'.

- Step 2** Click **Create**. The Create Task page appears as shown in [Figure 7-17](#).

Figure 7-10 The Create Task Page With Certificate Enrollment Audit Selected

The screenshot shows the 'Create Task' page in the Cisco IP Solution Center. The page is titled 'Create Task' and is part of a multi-step process (Step 1 of 2). The page shows a form for creating a task. The 'Name' field is 'Task Created 2003-06-17 13:17:40.157', the 'Type' is 'Certificate Enrollment Audit', and the 'Description' is 'Created on Tue Jun 17 13:17:40 PDT 2003'. The page is titled 'Create Task' and is part of a multi-step process (Step 1 of 2). The page shows a form for creating a task. The 'Name' field is 'Task Created 2003-06-17 13:17:40.157', the 'Type' is 'Certificate Enrollment Audit', and the 'Description' is 'Created on Tue Jun 17 13:17:40 PDT 2003'. The page is titled 'Create Task' and is part of a multi-step process (Step 1 of 2).

- Step 3 Select **Certificate Enrollment Audit** from the **Type** drop-down list.
- Step 4 Click **Next**. The Task Service Requests page appears as shown in Figure 7-18.

Figure 7-11 The Tasks Service Request Page

The screenshot shows the 'Task Service Requests' page in the Cisco IP Solution Center. The page is titled 'Task Service Requests' and is part of a multi-step process (Step 1 of 3). The page shows a table for displaying service requests. The table has columns for '#', 'Job ID', 'State', 'Type', 'Customer', and 'VPN'. The page is titled 'Task Service Requests' and is part of a multi-step process (Step 1 of 3). The page shows a table for displaying service requests. The table has columns for '#', 'Job ID', 'State', 'Type', 'Customer', and 'VPN'. The page is titled 'Task Service Requests' and is part of a multi-step process (Step 1 of 3).

- Step 5 Click **Add**. The Service Request for Task dialog box appears as shown in Figure 7-19.

**Note**

Only site-to-site and remote access service requests are available for certificate enrollment audits so, if present, they are the only service requests displayed in the Service Request for Task dialog box.

Figure 7-12 Service Request for Task Dialog Box

#	<input type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name
1.	<input type="checkbox"/>	5	PENDING	IPsec	ADD	admin	Customer2
2.	<input checked="" type="checkbox"/>	6	REQUESTED	IPsec RA	ADD	admin	Customer2

Rows per page: 10

Select Cancel

Step 6 Check the service request you want to audit and click **Select** to return to the Tasks Service Request page. The service request you checked now appears on the Tasks Service Request page.

Step 7 Click **Next**. The Task Schedules page appears as shown in [Figure 7-20](#).

Figure 7-13 The Task Schedules Page

You Are Here: Monitoring > Task Manager > Tasks

Mode: ADDING

- 1. SRs
- 2. Schedule
- 3. Summary

Task Schedules

#	<input checked="" type="checkbox"/>	Schedule	Start Date and Time	End Date and Time	Max Runs	Max Instances
Showing 0 of 0 records						

Rows per page: 10

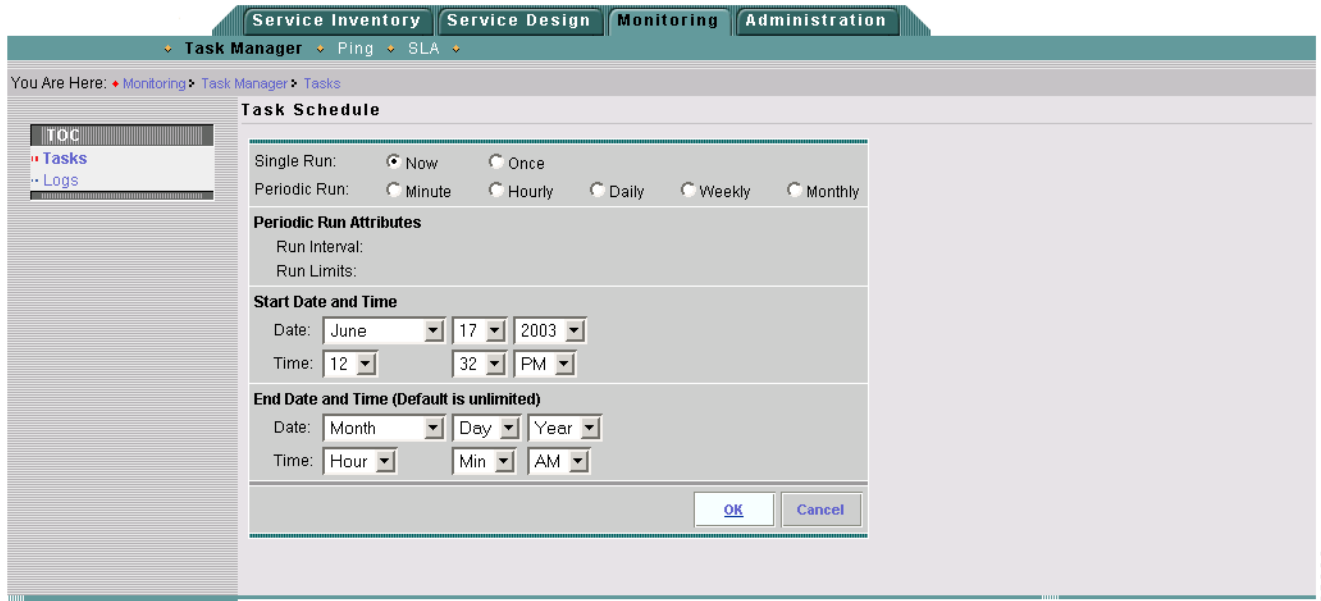
Create Delete

- Step 2 of 3 -

< Back Next > Finish Cancel

Step 8 Click **Create**. The Task Schedules page appears with the scheduling options displayed as shown in [Figure 7-21](#).

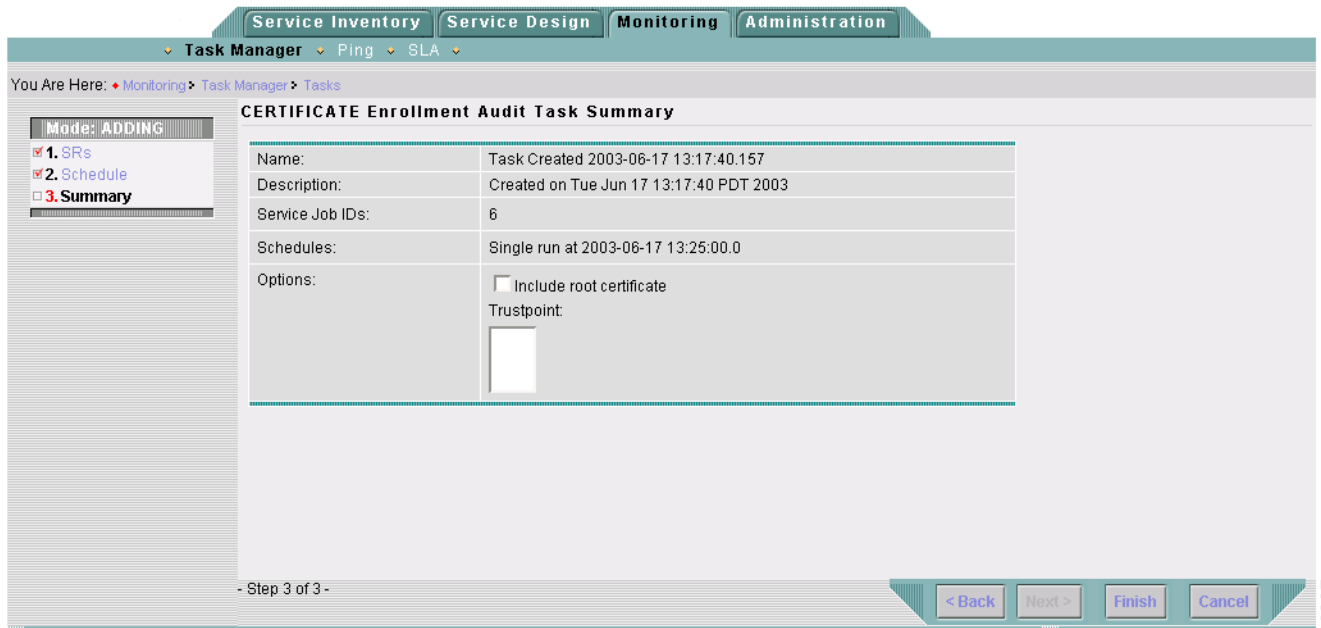
Figure 7-14 The Task Schedules With Scheduling Options Displayed



Step 9 Select when you would like the update to occur and click **OK** to continue.

Step 10 Click **Next**.

Figure 7-15 Certificate Enrollment Audit Task Summary Page



Step 11 Click **Finish** when done.

- Step 12** To view the results of the tasks you create, click **Home > Monitoring > Task Manager > Logs** and refer to the *Cisco IP Solution Center: Infrastructure Reference, 3.0* for information on logging options.

IPsec Functional Audits

An IPsec functional audit can be used after you deploy a service request to check the status of the VPN tunnels. The IPsec functional audit pings all the nodes of the VPN to check connectivity and ensure the tunnels are up.

IPsec functional audits can be performed for site-to-site and IPsec-to-MPLS service requests only.

- Step 1** To run an IPsec functional audit, click **Home > Monitoring > Task Manager > Tasks**. The Tasks page appears as shown in [Figure 7-16](#).

Figure 7-16 The Tasks Page

You Are Here: [Monitoring](#) > [Task Manager](#) > [Tasks](#)

Tasks

Show Tasks with Task Name matching of type

Showing 1-3 of 3 records

#	Task Name	Type	Schedule	Creator
1.	<input type="checkbox"/> c1	Collect Config	Single run at 2003-04-08 13:42:00.0	admin
2.	<input type="checkbox"/> Deployment Flow Task 2003-04-08 14:40:27.644	Deployment Flow	Single run at 2003-04-08 14:40:00.0	admin
3.	<input type="checkbox"/> Task Created 2003-06-10 16:44:15.292	Service Deployment	Single run at 2003-06-10 16:44:00.0	admin

Rows per page:

Auto Refresh:

93986

- Step 2** Click **Create**. The Create Task page appears as shown in [Figure 7-17](#).

Figure 7-17 The Create Task Page With IPsec Functional Audit Selected

Service Inventory Service Design Monitoring Administration

Task Manager Ping SLA

You Are Here: Monitoring > Task Manager > Tasks

Mode: ADDING

1. Create Task
2. ...

Create Task

Name*: Task Created 2003-06-17 12:50:33.58

Type: IPsec Functional Audit

Description: Created on Tue Jun 17 12:50:33 PDT 2003

Note: * - Required Field

- Step 1 of 2 -

< Back Next > Finish Cancel

93094

- Step 3** Select **IPsec Functional Audit** from the **Type** drop-down list.
- Step 4** Click **Next**. The Task Service Requests page appears as shown in Figure 7-18.

Figure 7-18 The Tasks Service Request Page

Service Inventory Service Design Monitoring Administration

Task Manager Ping SLA

You Are Here: Monitoring > Task Manager > Tasks

Mode: ADDING

1. SRs
2. Schedule
3. Summary

Task Service Requests

Show Services with Job ID matching * of type All Find

Showing 0 of 0 records

#	Job ID	State	Type	Customer	VPN
Rows per page: 10					

Add Delete

- Step 1 of 3 -

< Back Next > Finish Cancel

93988

- Step 5** Click **Add**. The Service Request for Task dialog box appears as shown in Figure 7-19.

Figure 7-19 Service Request for Task Dialog Box

#	<input type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name
1.	<input type="checkbox"/>	1	REQUESTED	QoS	ADD	admin	Customer1
2.	<input type="checkbox"/>	2	REQUESTED	MPLS	ADD	admin	Customer1
3.	<input type="checkbox"/>	3	FAILED_DEPLOY	L2VPN	ADD	admin	Customer1
4.	<input type="checkbox"/>	4	REQUESTED	Firewall	MODIFY	admin	Customer1
5.	<input checked="" type="checkbox"/>	5	REQUESTED	IPsec	ADD	admin	Customer2
6.	<input type="checkbox"/>	6	REQUESTED	IPsec RA	ADD	admin	Customer2
7.	<input type="checkbox"/>	7	REQUESTED	NAT	ADD	admin	Customer1

Showing 1-7 of 7 records

Rows per page: 10

Select Cancel

- Step 6** Check the service request you want to audit and click **Select** to return to the Tasks Service Request page. The service request you checked now appears on the Tasks Service Request page.
- Step 7** Click **Next**. The Task Schedules page appears as shown in Figure 7-20.

Figure 7-20 The Task Schedules Page

Service Inventory | Service Design | Monitoring | Administration

Task Manager | Ping | SLA

You Are Here: Monitoring > Task Manager > Tasks

Made: ADDING

- 1. SRs
- 2. Schedule
- 3. Summary

Task Schedules

Showing 0 of 0 records

#	<input checked="" type="checkbox"/>	Schedule	Start Date and Time	End Date and Time	Max Runs	Max Instances
---	-------------------------------------	----------	---------------------	-------------------	----------	---------------

Rows per page: 10

Create Delete

- Step 2 of 3 -

< Back | Next > | Finish | Cancel

- Step 8** Click **Create**. The Task Schedules page appears with the scheduling options displayed as shown in Figure 7-21.

Figure 7-21 The Task Schedules With Scheduling Options Displayed

Task Schedule

Single Run: Now Once

Periodic Run: Minute Hourly Daily Weekly Monthly

Periodic Run Attributes

Run Interval:

Run Limits:

Start Date and Time

Date: June 17 2003

Time: 12 32 PM

End Date and Time (Default is unlimited)

Date: Month Day Year

Time: Hour Min AM

OK Cancel

06666

Step 9 Select when you would like the update to occur and click **OK** to continue.

Step 10 Click **Next**. The IPsec Functional Audit Task Summary page appears as shown in Figure 7-22.

Figure 7-22 The IPsec Functional Audit Task Summary Page

IPsec Functional Audit Task Summary

Name:	Task Created 2003-06-17 12:50:33.58
Description:	Created on Tue Jun 17 12:50:33 PDT 2003
Service Job IDs:	5
Schedules:	Single run at 2003-06-17 13:12:00.0
Options:	<input type="checkbox"/> Mirror Pings <input checked="" type="checkbox"/> Verify all interfaces

- Step 3 of 3 -

< Back Next > Finish Cancel

98095

Step 11 Click **Finish** when done.

- Step 12** To view the results of the tasks you create, click **Home > Monitoring > Task Manager > Logs** and refer to the *Cisco IP Solution Center: Infrastructure Reference, 3.0* for information on logging options.

Viewing Task Logs

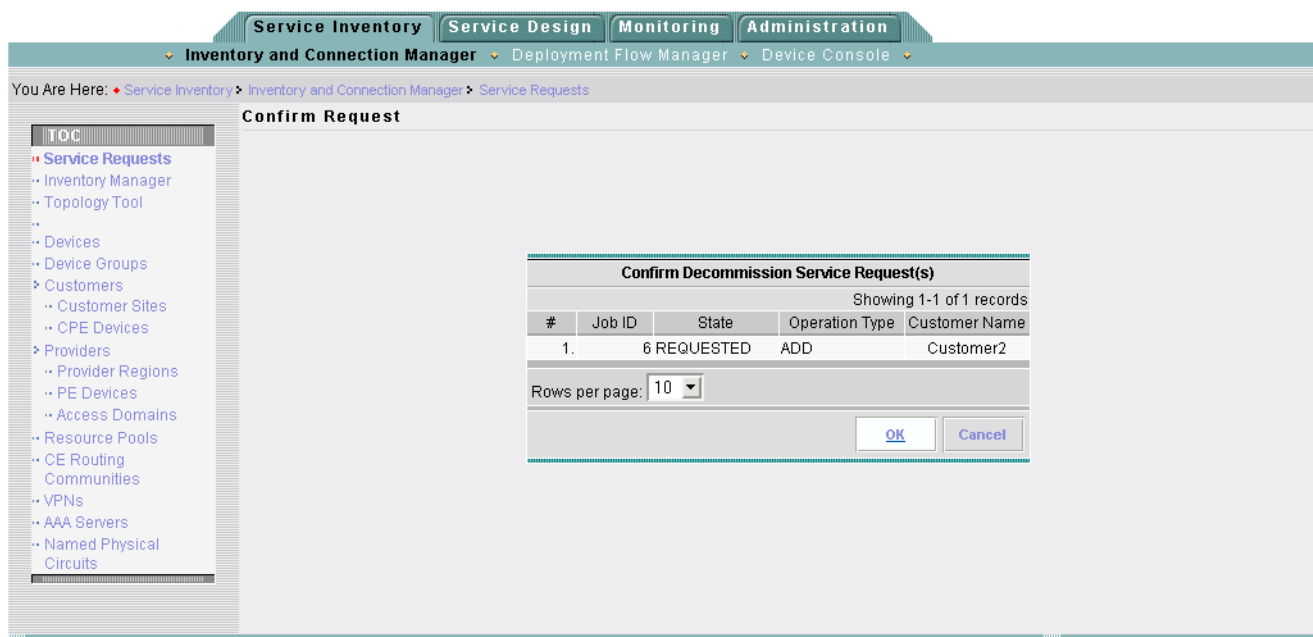
If more details are needed to troubleshoot a service request, view the task logs. To view the logs generated by the tasks you create, click **Home > Monitoring > Task Manager > Logs**. Please refer to the “Monitoring” chapter of the *Cisco IP Solution Center: Infrastructure Reference, 3.0* for more information on task logs.

Decommissioning a Service Request

Decommissioning a service request removes the security service from all CPE devices in the service request. To remove a security service, perform the following steps:

- Step 1** Click **Service Inventory > Inventory and Connection Manager > Service Requests**. The Service Requests page appears.
- Step 2** Put a check mark next to the service request you want to decommission.
- Step 3** Click **Decommission**. The Confirm Request page appears.

Figure 7-23 The Confirm Request Page



- Step 4** Click **OK** to confirm and decommission the service request, or click **Cancel** to return to the Service Requests page without decommissioning the service request.

**Note**

Notice on the Service Requests page, [Figure 7-24](#), the service request state is at REQUESTED. Also, in the **Operation Type** column, it is set to DELETE. The previous steps did not remove the service request; they only tagged it for deletion. To delete the service request, perform the steps below.

Figure 7-24 The Service Requests Page with a Service Request Pending Deletion

Service Requests

Show Services with Job ID matching * of type All Find

Showing 1-1 of 1 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	3	REQUESTED	IPsec RA	DELETE	admin	Customer1	Policy1	4/14/03 5:05 PM	

Rows per page: 10

Auto Refresh:

Create Details Edit Deploy Decommission Purge

Deploy Force Deploy

98132

Step 5 Put a check mark next to the service request with **Operation Type** DELETE.

Step 6 Click **Deploy**.

Step 7 Specify when you want ISC to remove the service request in the Deploy Service Requests page.

Step 8 Click **Save**. ISC creates the necessary removal configuration to delete the security service from the device(s). As part of the decommission process, ISC audits the configuration to ensure that the service is removed completely. Once audited, the service request state changes to a CLOSED state.

To release CPE devices and policies from the database, use the **Purge** option on the Service Requests page.

