



PROCESS OVERVIEW GUIDE

CISCO MONITORING AND REPORTING SERVICE ACTIVATION PROCESS OVERVIEW

Before you can begin using your Cisco® Monitoring and Reporting Service, the service needs to be activated. Service activation is a process to establish connectivity to support monitoring and provision the monitoring solution..

The monitoring solution is hosted by Cisco Systems®, and your help is needed to establish a VPN connection between Cisco and your network. To establish connectivity, you will receive a preconfigured Cisco 1800 Series Integrated Services Router to install in your network as a VPN termination device.

The complete activation process takes approximately 30 days. As illustrated in Figure 1, the customer is responsible for three sets of tasks and will work with a Cisco activation engineer to collect the information required to enable the service.

After receiving your completed [service activation kit](#), Cisco will require approximately 15 days to process the information and ship the VPN termination device. After the VPN termination device is installed, approximately 5 days are required to complete activation activities.

Figure 1 Activation Process



GETTING STARTED

After you receive a welcome e-mail from the Cisco activation team, please download the service activation kit. The kit is an Excel spreadsheet used to collect pertinent information about your Cisco Unified Communications applications. To complete the service activation kit, you will need information about your voice applications (for example, Cisco CallManager and Cisco Unity® server IP addresses) for Unified Communications, so it is best to fill it out after your Cisco Unified Communications system is installed. Return the completed kit to activation-team@cisco.com.

As part of the service activation process, you will be required to:

1. Download the [service activation kit](#).
2. Select a service installation option for the VPN termination device provided by Cisco.
3. Complete and return the service activation kit to the Cisco activation team (activation-team@cisco.com).
4. Install the VPN termination device in your network. This device will be used to terminate secure monitoring access (IP Security [IPsec] VPN) to your Cisco Unified CallManager, Cisco Unity, and/or Cisco Unity connection servers.
5. Change the default cluster ID name on your Cisco Unified CallManager, Cisco Unity, and/or Cisco Unity Connection servers to another name (if you have not done so already).
6. Make changes to your firewall to enable the secure monitoring connection.
7. Add routes to your network to help ensure that traffic from Cisco Unified Communications servers is directed to the secure monitoring connection.
8. Contact Cisco at 888 676-6440 and notify the service activation team that the VPN termination device has been installed and the required network updates have been made.

After the secure connection for monitoring has been tested and activated, you will receive an e-mail from Cisco with the URL and credentials for accessing your Cisco Monitoring and Reporting Service dashboard. The dashboard provides access to your alerts and reports.

SERVICE INSTALLATION OPTIONS

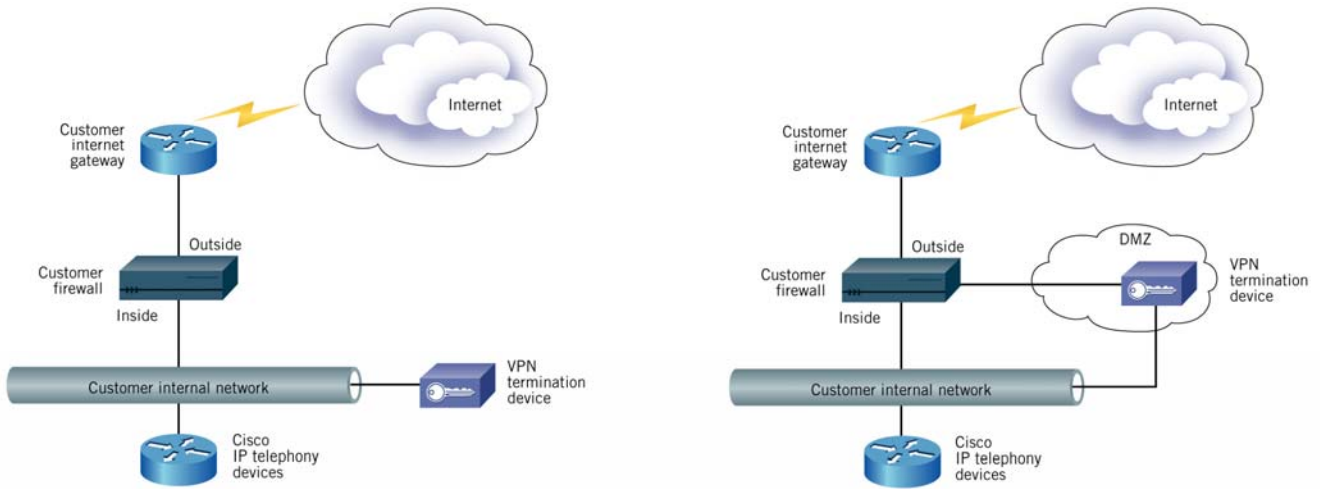
Cisco uses the information you provide in the service activation kit to configure the monitoring capability in the Cisco Monitoring and Reporting Service. After you have downloaded the service activation kit, you need to fill out each worksheet completely. This means you will need specific information about your Cisco Unified Communications applications, including server IP addresses and security credentials.

You will also need to assign up to two IP addresses from your network for the Cisco VPN termination device. These IP addresses will be assigned to a VPN termination device, which Cisco will ship to you. This device is used to terminate the secure VPN connecting your network to the Cisco Remote Operations Services management network.

VPN TERMINATION DEVICE INSTALLATION OPTIONS

There are two deployment options for the VPN termination device (Figure 2). The option you choose largely depends on your network configuration. If you currently have a demilitarized zone (DMZ), Cisco recommends that you choose to place the VPN termination device within the DMZ (option 2). If you do not have a DMZ, then option 1 will work better for you. The option you choose will determine the specific IP addresses that you assign to the VPN termination device.

Figure 2 Deployment Options



Option 1 – VPN termination device inside the firewall

Option 2 – VPN termination device inside the DMZ

Whether you choose option one or two, you will need to provide a public IP address for the router. This IP address can be assigned either to the WAN port of the router itself (option 2), or implemented on your internet gateway or firewall (option 1 or 2). If you choose to implement the public address on your gateway router or firewall, it will need to be mapped 1-1 to the NAT address assigned to the router.

For option 1 you will need to provide:

- Your default gateway IP address
- The IP address you want to assign to the VPN termination device
- A public IP address (if the IP address that you assign to the VPN device is a NAT [private] address)

For option 2 you will need to provide:

- Your default gateway IP address
- The IP address you want to assign to the VPN termination device's public/outside port
- The IP address you want to assign to the VPN termination device's private/inside port
- A public IP address (if the IP address that you assign to the VPN device is a NAT [private] address)
- An IP address for the default gateway to the IPC devices

Please include these assignments in the information you send back to Cisco in the Service Activation Kit.

Both deployment options assume the following about your existing network infrastructure:

- Your internet gateway and firewall will forward IPsec packets to the Cisco VPN termination device.

- Your Internet router is not configured to use Network Address Translation (NAT) to your firewall.
- Your firewall is configured to use NAT to your internal network.

In both alternatives you will need to open Internet Security Association and Key Management Protocol (ISAKMP), Encapsulating Security Protocol (ESP) and User Datagram Protocol (UDP) 4500 ports through your firewall. You might want to add access control to restrict communications of the VPN termination device to Cisco Unified Communications servers for Simple Network Management Protocol (SNMP) and HTTP services.

If your network infrastructure is configured in a manner other than that just described, contact Cisco at 888 676-6440 or by e-mail at activation-team@cisco.com for assistance with alternate configuration options.

After you have decided which option works better for you, complete the [service activation kit](#) and e-mail it to activation-team@cisco.com.

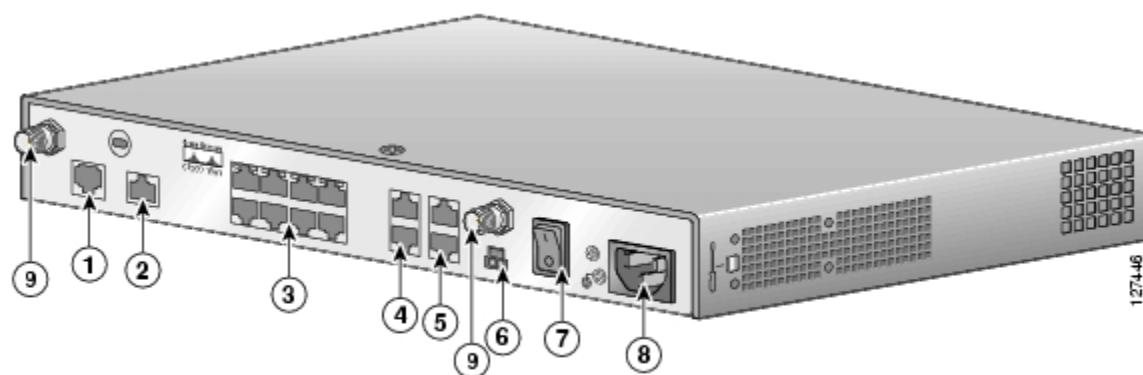
Installing the Cisco 1800 As A VPN Termination Device

Within 15 days of sending the completed [service activation kit](#) back to Cisco, you will receive a Cisco 1800 Series Integrated Services Router VPN termination device by FedEx. The VPN termination device will be preconfigured for deployment within your network.

Note: This router is the property of Cisco Systems and is to be used solely for the Cisco Monitoring and Reporting Service.

Cisco will use this router to terminate secure monitoring access (IPsec VPN) to your Cisco Unified Communications servers. The use of the Cisco 1800 Series Integrated Services Router (Figure 3) to provide monitoring connectivity to your Unified Communications servers is a requirement for this service.

Figure 3 Back Panel of Cisco 1800 Series Integrated Services Router



1 Asymmetric DSL (ADSL) over basic telephone service WAN port	6 Power over Ethernet (PoE) connector ¹
---------------------------------------------------------------	----------------------------------------------------

2	ISDN Basic Rate Interface (BRI) S/T port	7	Power switch
3	Managed 8-port Fast Ethernet switch	8	Power connector
4	Fast Ethernet WAN port	9	RP-TNC antenna connectors (wireless models only)
5	Console and auxiliary ports		

⁴Inline power is a field-upgradable option only. It is not installed by default.

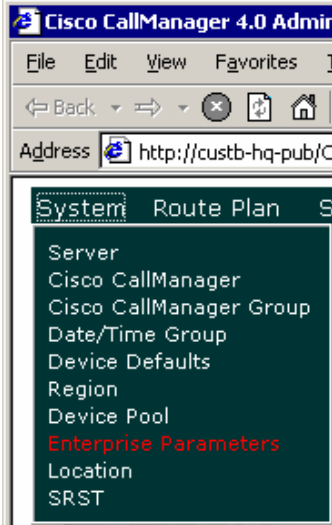
1. Upon receipt of the router, unpack the contents of the box, which should include:
 - Cisco 1800 Integrated Services Router
 - AC power cord
 - Device documentation
2. Place the router in a communications rack, which will allow for easy access to both 120VAC AC power and the necessary network infrastructure to which the Cisco 1800 will be connected.
3. Connect the router's AC power to a 15A, 120VAC (10A, 240VAC circuit with overcurrent protection). (Note: The input voltage tolerance limits for AC power are 90 and 264VAC.)
4. Connect one end of an Ethernet cable to the Fast Ethernet WAN port (item 4 in Figure 3) of the Cisco 1811. Connect the other end of the Ethernet cable to your WAN access device (per your deployment location decision made prior to completing the [service activation kit](#)).
5. If you are deploying the VPN termination device in your DMZ, connect one end of an Ethernet cable to port 1 on the eight-port switch on the Cisco 1800 Integrated Services Router (item 3 in Figure 3). Connect the other end of the Ethernet cable to your LAN access device.

Change Cisco Unified CallManager and Cisco Unity Server Cluster ID

Cisco Unified CallManager and Cisco Unity servers come with a default cluster ID value. The Cisco Monitoring and Reporting Service requires that the factory default name on each server be changed to some other name. We suggest that you use your company and location to construct a new cluster ID. After you have renamed all of the Cisco Unified Communications servers, enter the new names in the Cluster ID field in the IPC Devices table provided in the [service activation kit](#). Follow these steps to change the cluster ID:

1. Log in to Cisco CallManager Publisher and go to System > Enterprise Parameters (Figure 4).

Figure 4 Changing Default Cluster IDs



2. The factory default cluster ID is “StandAloneCluster.” Rename the cluster using your company name and site name. For example, if your company is ACME Systems and you are located in Phoenix, Arizona, change the cluster ID to ACMESys-PHX. If you have multiple locations within the same city, use location names that are meaningful to you (for example, downtown, airport, Oak Street, and so on). You can be as descriptive as you want to be (Figure 5).

Figure 5 Sample Cluster ID



Configure Your Firewall

Open ISAKMP, ESP, UDP 161 SNMP, UDP 4500, and TCP 80, 443 ports on your firewall. If your firewall is stateful, you should not need to add any static routes. If you are using a nonstateful firewall, then you might need to add routes to help ensure that Cisco Unified Communications servers route to the VPN termination device.

Configure Your Network

Both alternatives will require you to add static routes to your network to help ensure that traffic from the Cisco Unified Communications servers is routed through the VPN termination device. Install the routes as needed in your network.

You might also want to restrict traffic between the Cisco VPN termination device to just the Cisco Unified Communications servers for HTTP and SNMP services.

Contact the Cisco Activation Team

After the VPN termination device has been properly installed in your network and you have made the required firewall changes and added any new static routes to your network, call the Cisco activation team at 888 676-6440 or contact the team by e-mail at activation-team@cisco.com. The activation team will schedule an activation session with you to remotely verify connectivity to your Cisco Unified Communications servers, complete your installation, and activate the service.

Cisco will notify you when your installation is complete and give you the URL for your monitoring dashboard, in addition to your security credentials. At that point you will be able to access the Cisco Monitoring and Reporting Service dashboard and use the online capabilities that it offers for monitoring your Cisco Unified Communications system.

For Assistance with Service Activation

For assistance with service activation, please contact the Cisco activation team:

- E-mail: activation-team@cisco.com
- Phone: 888 676-6440

For Assistance After Your Service Has Been Installed and Activated

For assistance accessing your Cisco Monitoring and Reporting Service dashboard or questions about how to use it, call the Cisco Monitoring and Reporting Service helpdesk at 800 553-2447.

For questions about resolving specific alerts, events logged on your Cisco Monitoring and Reporting Service dashboard, or general questions about Cisco Unified Communications issues or configurations:

- Refer to the technical support documentation located at www.cisco.com/en/US/partner/products/sw/voicesw/tsd_products_support_category_home.html,
- Open a TAC service request using the online form located at <http://tools.cisco.com/ServiceRequestTool/create>.



the Cisco Web site at [Hwww.cisco.com/go/officesH](http://www.cisco.com/go/offices).