



Opening a Case With TAC

When you open a case with the Cisco TAC, you must provide preliminary information to better identify and qualify the issue. You may need to provide additional information, depending on the nature of the issue. Waiting to collect the following information upon the engineer's request after opening a case inevitably results in resolution delay.

- [Required Preliminary Information](#)
 - [Network Layout](#)
 - [Problem Description](#)
 - [General Information](#)
- [TAC Web](#)
- [CCO Cases](#)
- [Attachments](#)
- [Cisco Live!](#)
- [Remote Access](#)

Required Preliminary Information

For all issues, always provide the following information to TAC. Collect and save this information for use upon opening a TAC case and update it regularly with any changes.

- [Network Layout](#)

- [Problem Description](#)
- [General Information](#)

Network Layout

A detailed description of the physical and logical setup, as well as all the following network elements involved in the voice network (if applicable):

- Cisco CallManager(s)
 - Version (from Cisco CallManager Administration choose **Details**)
 - Number of Cisco CallManagers
 - Setup (stand-alone, cluster)
- Unity
 - Version (from the Cisco CallManager Administration)
 - Integration type
- Applications
 - List of installed applications
 - Version numbers of each application
- IP/voice gateways
 - OS version
 - Show tech (IOS gateway)
 - Cisco CallManager load (Skinny gateway)
- Switch
 - OS version
 - VLAN configuration
- Dial plan—Numbering scheme, call routing

Ideally, submit a Visio or other detailed diagram, such as JPG. Using the whiteboard, you may also provide the diagram through a Cisco Live! session.

Problem Description

Provide step-by-step detail of actions that the user performed when the issue occurs. Ensure the detailed information includes

- Expected behavior
- Detailed observed behavior

General Information

Make sure that the following information is readily available:

- Is this a new installation?
- If this is a previous version of a Cisco CallManager installation, has this issue occurred since the beginning? (If not, what changes were recently made to the system?)
- Is the issue reproducible?
 - If reproducible, is it under normal or special circumstances?
 - If not reproducible, is there anything special about when it does occur?
 - What is the frequency of occurrence?
- What are the affected devices?
 - If specific devices are affected (not random), what do they have in common?
 - Include DNs or IP addresses (if gateways) for all devices that are involved in the problem.
- What devices are on the Call-Path (if applicable)?

TAC Web

Use TAC Web, a detailed collection of tools and technical documents written by TAC engineers, to analyze common issues and provide solutions. See the presentation covering TAC Web tools and content that is available to help you use this tool at the following URL:

<http://www.cisco.com/public/support/tac/home.shtml>

CCO Cases

Opening a case through CCO gives it priority over all other case-opening methods. High priority cases (P1 and P2) provide an exception to this rule.

Provide an accurate problem description when opening a CCO case. That description of the problem returns URL links that may provide you with an immediate solution.

If you do not find a solution to your problem, continue the process of sending your case to a TAC engineer.

Attachments

Attach reports to a case by sending an email to the engineer and attaching a zip file for documents larger than 100 Kb.

At the following URL, use the *Manage a TAC Case* section, *please login* link to log in as a registered user:

<http://www.cisco.com/public/support/tac/contact.shtml>

Cisco Live!

Cisco Live!, a secure, encrypted Java applet, allows you and your Cisco TAC engineer to work together more effectively by using Collaborative Web Browsing / URL sharing, whiteboard, Telnet, and clipboard tools.

Access Cisco Live! at the following URL:

<http://c3.cisco.com/>

Remote Access

Remote access provides you with the ability to establish Terminal Services (remote port 3389), HTTP (remote port 80), and Telnet (remote port 23) sessions to all the necessary equipment.



Caution

When setting up dial-in, do not use **login:cisco** or **password:cisco** because they constitute a vulnerability to the system.

You may resolve many issues very quickly by allowing the TAC engineer remote access to the devices through one of the following methods:

- Equipment with public IP address.
- Dial-in access—In decreasing order of preference: analog modem, Integrated Services Digital Network (ISDN) modem, virtual private network (VPN).
- Network Address Translation (NAT)—IOS and private Internet exchange (PIX) to allow access to equipment with private IP addresses.

Ensure that firewalls do not obstruct IOS traffic and PIX traffic during engineer intervention and that all necessary services, such as Terminal Services, start on the servers.



Note

TAC handles all access information with the utmost discretion, and no changes will be made to the system without customer consent.

Cisco Secure Telnet

Cisco Secure Telnet offers Cisco Service Engineers (CSE) transparent firewall access to Cisco CallManager servers on your site.

Cisco Secure Telnet works by enabling a Telnet client inside the Cisco Systems firewall to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and maintenance of your Cisco CallManager servers without requiring firewall modifications.

**Note**

Cisco accesses your network only with your permission. You must provide a network administrator at your site to help initiate the process.

Firewall Protection

Virtually all internal networks use firewall applications to restrict outside access to internal host systems. These applications protect your network by restricting IP connections between the network and the public internet.

Firewalls work by automatically blocking TCP/IP connections that are initiated from the outside, unless the software is reconfigured to allow such access.

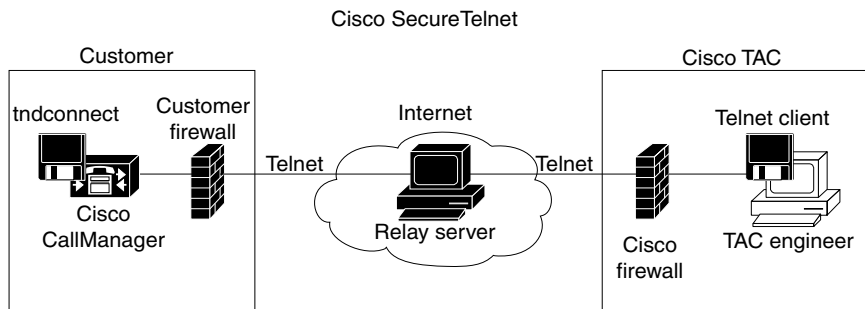
Corporate networks normally permit communication with the public Internet but only if connections directed to outside hosts originate from inside the firewall.

Cisco Secure Telnet Design

Cisco Secure Telnet takes advantage of the fact that Telnet connections can easily be initiated from behind a firewall. Using an external proxy machine, the system relays TCP/IP communications from behind your firewall to a host behind another firewall at the Cisco Technical Assistance Center (TAC).

Using this relay server maintains the integrity of both firewalls while supporting secure communication between the shielded remote systems.

Figure A-1 Cisco Secure Telnet System



34483

Cisco Secure Telnet Structure

The external relay server establishes the connection between your network and Cisco Systems by building a Telnet tunnel. This enables you to transmit the IP address and password identifier of your Cisco CallManager server to your CSE.



Note

The password comprises a text string upon which your administrator and the CSE mutually agree.

Your administrator starts the process by initiating the Telnet tunnel, which establishes a TCP connection from inside your firewall out to the relay server on the public Internet. The Telnet tunnel then establishes another connection to your local Telnet server, creating a two-way link between the entities.



Note

The Telnet client at the Cisco TAC runs in compliance with systems running on Windows NT and Windows 2000 or with UNIX operating systems.

After the Cisco CallManager at your site accepts the password, the Telnet client that is running at the Cisco TAC connects to the Telnet daemon that is running behind your firewall. The resulting transparent connection allows the same access as if the machine were being used locally.

Once the Telnet connection is stable, the CSE can implement all remote serviceability functionality to perform maintenance, diagnostic, and troubleshooting tasks on your Cisco CallManager server.

You can view the commands sent by the CSE and the responses issued by your Cisco CallManager server, but the commands and responses may not always be completely formatted.

Where to Find More Information

For detailed information, refer to the *Cisco CallManager Serviceability Administration Guide*.

