

CallManager Approved Methods for Remote Cisco Technical Support Access

Document ID: 63625

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Approved Remote Access Methods

- Cisco CallManager
- VNC
- WTS (Remote Desktop)
- Integrated Lights Out (ILO)
- Cisco MeetingPlace

Secure Network Connections

- How to Use a VPN

Related Information

Introduction

In addition to the Remote Access procedures listed in the Installing the Operating System on the Cisco IP Telephony Applications Server, this document lists the methods used by Cisco Technical Support to access systems remotely. This greatly enhances the engineer's ability to diagnose and resolve system issues. Though it is not required, customers are highly encouraged to supply some kind of access for troubleshooting purposes.

It is the customer's responsibility to supply any required software.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco CallManager 3.x(x) and later
- Virtual Network Computing (VNC)
- Windows Terminal Service (WTS) (also called Remote Desktop)
- Cisco MeetingPlace

WTS is not supplied by Cisco.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Approved Remote Access Methods

Cisco CallManager

For additional information on Cisco CallManager remote access, refer to the May I use Terminal Services, VNC, or ILO on this server during the upgrade chapter of *Installing the Operating System on the Cisco IP Telephony Applications Server, Version 2000.2.6*.

VNC

VNC now ships with the Cisco CallManager install CD and is supported for remote access to Cisco CallManager. For more information on VNC, refer to the RealVNC site .

VNC is the only supported remote access method for software installations and upgrades.

If you want to use Virtual Network Computing (VNC) to remotely upgrade a Cisco CallManager server, refer to the Cisco IP Telephony Operating System documentation page to obtain the latest version of the VNC document.

For more information, refer to Upgrading Cisco CallManager Release 4.1.2.



Caution: If you have installed VNC but do not plan to use it to perform the upgrade, disable it to prevent remote access to the server. If you do not disable VNC and a user/administrator accesses the server at the time of the upgrade, the upgrade fails.

WTS (Remote Desktop)

Cisco installs Terminal Services. Therefore, Cisco Technical Support is able to perform remote administration and troubleshooting tasks. Windows Terminal Services is supported and preferred for remote server administration and access for Cisco Technical Support.

WTS Limitations

Installation or upgrades of software is not supported on Cisco CallManager.



Caution: Before the upgrade, Cisco recommends that you disable Terminal Services and immediately reboot the server to prevent remote access to the server. If you access the server through Terminal Services, it sometimes causes the upgrade to fail.

After you upgrade the server, you must enable Terminal Services.

For more information on WTS, refer to Microsoft's WTS site .

Integrated Lights Out (ILO)

Do not use ILO to perform upgrade or installation tasks. Cisco supports ILO for remote management and

configuration tasks only.

For more information on ILO, refer to About ILO.

Cisco MeetingPlace

Cisco MeetingPlace is a unique tool used by Technical Support for web conferencing. It allows access to systems through HTTP. As long as there is Internet access from the Cisco CallManager server, this is the preferred method.

Note: By default, Internet Explorer opens new links in the existing windows. Therefore, you can easily lose your web conference when you click on a link. To prevent this Internet Explorer behavior, select **Tools > Internet Options > Advanced** and uncheck **Reuse windows for launching shortcuts**.

Open TCP port 1627 in order to share the desktop. If TCP port 1627 is blocked by the firewall, messages are tunneled through TCP port 80. Cisco MeetingPlace also supports tunneling using HTTPS (SSL). SSL requires an SSL Certificate. To enable support for SSL, port 443 must be open on the network. For information on the Web Conferencing application, refer to Cisco MeetingPlace Web Conferencing.

Note: When you initiate a Terminal Service session to the Cisco CallManager server, launch a browser from there to Cisco MeetingPlace, share the desktop, and then minimize this Terminal Service session, the web conference with Technical Support freezes. Cisco recommends that you either share the desktop from your local PC, logon to Cisco MeetingPlace from the server console directly, or do not minimize your Terminal Service session to the Cisco CallManager.

For additional product information, refer to Cisco MeetingPlace.

If you need to set up a session with a Technical Support engineer, go to the TAC MeetingPlace page.



To attend to a meeting, enter the Meeting ID above and click on the Attend Meeting button. For assistance or to learn more about what MeetingPlace can do for you, click Help.



First time users should run the [Browser Test](#) to verify you can participate in a web conference.
Copyright © 1996-2005 [Latitude Communications](#). All Rights Reserved. Version: 4.3.0.248.5
MeetingPlace and MeetingNotes are trademarks of Latitude Communications.

From this page, enter the unique meeting ID number that the Technical Support engineer assigns for this meeting. If you are a first time user, select the Browser Test link to ensure compatibility. If you do not already have them, the Test Browser page prompts you to install some Java components. This is a one time process. It is not required the next time you connect to Cisco MeetingPlace.

Once you sign in as a guest, you can share any application with the Technical Support engineer and allow the engineer control.

Note: When you use Cisco MeetingPlace for Web Conferencing, the Internet browser process uses a portion of CPU resources. This is expected behavior.

Secure Network Connections

Customers are responsible for secure network connectivity for access. Cisco Virtual Private Network (VPN) connections are the preferred method.

How to Use a VPN

A VPN is a private network that uses public phone lines (or in some cases a cable modem). Privacy is maintained through encryption and the use of secure protocols. When you use a VPN to access Cisco CallManager through a firewall, you can use Cisco CallManager as if you were inside the network.

VPN is required in these circumstances:

- When you need access to the Cisco CallManager website (<http://<Cisco CallManager server name>/ccmadmin>) from a remote computer outside your network firewall.

Note: If you do not use VPN for remote access, refer to the Microsoft website for information on configuring Distributed Component Object Model (DCOM) through a firewall.

Discuss the set up of a VPN with your LAN administrator.

Related Information

- [Voice Technology Support](#)
- [Voice and IP Communications Product Support](#)
- [Recommended Reading: Troubleshooting Cisco IP Telephony](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Nov 20, 2007

Document ID: 63625
