

Cisco Unified MeetingPlace Web Conferencing System: Require Client Certificates in IIS

Document ID: 71504

Introduction

Prerequisites

Requirements

Components Used

Conventions

Task List

Configure IIS to Require Client Certificates

Install the Client Certificate on the Web Conferencing Server

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

For increased security, you can require client certificates for Cisco Unified MeetingPlace Web Conferencing. This document describes how to require client certificates for Cisco Unified MeetingPlace Web Conferencing.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt the procedures in this document:

- Install and configure Cisco Unified MeetingPlace Web Conferencing Release 5.4.
- Obtain a client certificate.
- Export the client certificate to a .pfx file.
- Install the client certificate on the clients for all users.
- Install your Secure Socket Layer (SSL) certificate on the Web Conferencing server.

Components Used

Cisco Unified MeetingPlace Web Conferencing Release 5.4

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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Task List

Do these tasks in the order listed in order to require client certificates in Internet Information Services (IIS) for Cisco Unified MeetingPlace Web Conferencing.

1. Configure IIS to require the client certificates.
2. Install the client certificate on the Web Conferencing server.

Configure IIS to Require Client Certificates

Complete these steps in order to configure IIS to require client certificates.

1. Go to the Windows **Start** menu and choose **Programs > Administrative Tools > Internet Services Manager**.
2. In the left pane of the Internet Information Services window, expand the **Web Conferencing** server and click **Default Web Site**.
3. In the right pane, right-click the web site and select **Properties**.
4. In the Properties dialog box, go to the Directory Security tab.
5. Under Secure Communications, click **Edit**.
6. In the Edit dialog box, check the **Require Client Certificates** check box and click **OK**.
7. In the Properties dialog box, click **OK**.
8. Close the Internet Information Services window.

Install the Client Certificate on the Web Conferencing Server

Internally, the Web Conferencing server uses HTTP or HTTPS to connect back to itself to start web conferences. Because client certificates are required, you must also give the Web Conferencing server a client certificate, which can be any user's client certificate or a client certificate that is specifically provisioned for the Web Conferencing server.

Note: Ensure that you have already exported the client certificate to a .pfx file and saved the file to the Web Conferencing server.

1. Choose **Start** and click **Run**.
2. In the Open field of the Run dialog box, enter **MMC.exe** and click **OK**.
3. From the **File** menu, click **Add/Remove Snap-in**.
4. Click **Add** in the Add/Remove Snap-in dialog box.
5. In the Add Standalone Snap-in dialog box, choose **Certificates** and click **Add**.
6. On the Certificates Snap-in page, choose **Server Account** and click **Next**.
7. Choose **Local Computer** and click **Next**.
8. Choose **Cisco MeetingPlace Agent Service** and click **Finish**.
9. In the Add/Remove Snap-in dialog box, click **OK**.
10. In the left pane, fully expand the node for the server.
11. Right-click **MPAgent/Personal** and choose **All Tasks > Import**.
12. Click **Next**.
13. Enter the file name of the .pfx file that is saved to the Web Conferencing server and click **Next**.
14. Accept the default settings and click **Next**.



Caution: Do not enter a password or check the **Mark This Key as Exportable** check box.

Otherwise, the client certificate feature does not function correctly.

15. Accept the default settings and click **Next**.
16. Click **Finish**.
17. Click the **Certificate** node, and confirm that there is only one client certificate. If more than one certificate is in this node, the client certificate feature does not function correctly.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Voice
Service Providers: Voice over IP
Voice & Video: Voice over IP
Voice & Video: IP Telephony
Voice & Video: IP Phone Services for End Users
Voice & Video: Unified Communications
Voice & Video: IP Phone Services for Developers
Voice & Video: General

Related Information

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

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Feb 23, 2007

Document ID: 71504
