Main page: Cisco Unified MeetingPlace, Release 8.0

Up one level: Configuration

Note: This topic does *not* apply to deployments in which users schedule meetings from the Cisco WebEx site. For information about Cisco WebEx integration deployments, see the *Planning Guide for Cisco Unified MeetingPlace* at http://docwiki.cisco.com/wiki/Cisco_Unified_MeetingPlace%2C_Release_8.0_--_Planning_Your_Deployment.

This module describes how to enable external users to access meetings, meeting data, and recordings by configuring your Cisco Unified MeetingPlace system to use two Web Servers or two clusters of Web Servers. One is on the internal network, behind the firewall; the other is on another network segment, such as a DMZ. The internal server or cluster is accessible only from behind the firewall, while the external server or cluster is accessible from inside or outside the firewall. This deployment is called Segmented Meeting Access-2 Servers (SMA-2S).

- Restrictions for Accessing Meeting Data from an External (DMZ) Web Server
- Prerequisites for Configuring SMA-2S
- Configuring SMA-2S
- How to Test Your SMA-2S Configuration

Contents

Restrictions for Accessing Meeting Data from an External (DMZ) Web Server

External users can access meeting details and recordings only within the first 24 hours after the meeting has

ended. External users can access this meeting data on the external Web Server by doing one of the following:

- Using the click-to-attend link in the meeting notification.
- Entering the Meeting ID in the web user portal on the external Web Server.

Meeting data is available for a longer period to profiled users from the *internal* Web Server, depending on how the Days until meeting statistics deleted field on the Meeting Configuration Page was configured at the time the meeting was scheduled.

Related Topics

- Table: Field Reference: Meeting Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace (M - P pages)
- Configuring Segmented Meeting Access for Cisco Unified MeetingPlace module

Prerequisites for Configuring SMA-2S

Before you configure SMA-2S, make sure that you install the Cisco Unified MeetingPlace Web Server software specifically for an SMA-2S deployment on both the internal and external Web Servers.

See the Installing the Cisco Unified MeetingPlace Web Server Software in a Segmented Meeting Access (SMA-2S) Configuration module.

Note: If you have Cisco Security Agent running, SSH access to the external Web Server will be blocked. You may want to consider other access modules, such as VNC or Remote Desktop, to provide access to the external Web Server.

What to Do Next

Proceed to the Configuring SMA-2S.

Configuring SMA-2S

External meetings are held on an external Web Server so that users can access their meetings from the Internet. Rather than have all of your users sign in to a particular external Web Server, configure automatic redirection of all external meetings from your internal Web Servers to a designated external Web Server.

Before You Begin

Complete the Prerequisites for Configuring SMA-2S.

Procedure

1. Sign in to the web user portal on the internal Web Server.
2. Select **Admin**.
3. Select **Web Server**.
4. From a blank Web Server Name field, enter the name of a new Web Server to represent your designated external Web Server.
5. Enter the fully qualified domain name (FQDN) of your external Web Server in the Hostname field, that is, *hostname.domain.com*. If your Web Server is not in a Domain Name Server (DNS), enter the IP address instead.
   - ♦ You must be able to resolve this hostname from the internal Web Server.
   - ♦ If you are using SSL, make sure that the hostname on the SSL certificate resolves to the external Web Server IP address.
   - ♦ If you are using SSL and a segmented DNS, make sure that the DNS name and the SSL certificate name differ.
6. Select **Submit** to add this Web Server to the database.
   This server now appears as part of your list of Web Servers in the "View" section of the page.
7. Return to the main Administration page and select **Site**.
8. Select the Site Name that represents your cluster of internal Web Servers.
   Note: Site Name should have a default value equal to the NetBIO name of the first Web Server you installed in this cluster.
9. Select the external Web Server you just added for DMZ Web Server.
   This configures the internal Web Servers in this cluster to point to this external Web Server in the case of external meetings.
10. Select **Submit**.
    Tip: The external cluster does not require any additional SQL Server database configurations.

What to Do Next

Proceed to How to Test Your SMA-2S Configuration.

How to Test Your SMA-2S Configuration

- Testing Internal Meetings
- Testing External Meetings

Testing Internal Meetings

Before You Begin

Complete the Configuring SMA-2S.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Schedule a meeting with internal access.
    1. From the Welcome page, select **Schedule Meeting**.
    2. Set your meeting details, including meeting date and time.
    3. Select **No** for **Allow External Web Participants**.
    4. Select **Schedule**.
3. Verify that you received a notification for the meeting you scheduled in Step 2.
4. From the Internet, verify that the internal click-to-attend link in your notification does *not* work by clicking the link.
5. From inside the private corporate network, verify that the internal click-to-attend link in your notification works by clicking the link.
6. If a Cisco WebEx web meeting is automatically launched, then proceed to Step 11.
7. If the Cisco Unified MeetingPlace web user portal appears, then proceed to Step 8.
8. Enter the meeting ID and select **Attend Meeting**.
9. Verify that you can dial in to the voice meeting by using the "Phone dial-in" and "Meeting ID" values that appear.

    The remaining steps apply only if your system is integrated with Cisco WebEx.
10. Select **Connect** to join the web meeting.
11. Follow the prompts to join the web meeting.
12. If prompted to enter your phone number, then verify that you can join the voice meeting via a dial-out call.
13. Verify that you are signed in as your profile by making sure that your profile name appears in the web meeting room.

What to Do Next

Proceed to the Testing External Meetings.

Testing External Meetings

Before You Begin

Complete the Testing Internal Meetings.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Schedule a meeting with external access by completing the following steps:
    1. From the Welcome page, select **Schedule Meeting**.
    2. Set your meeting details, including your meeting date and time.
    3. Select **Yes** for Allow External Web Participants.
    4. Select **Schedule**.
3. Verify that you received a notification for the meeting you scheduled in Step 2.
4. From the Internet, verify that the external click-to-attend link in your notification works by clicking the link.
5. If a Cisco WebEx web meeting is automatically launched, then proceed to Step 10.
6. If the Cisco Unified MeetingPlace web user portal appears, then proceed to Step 7.

7. Enter the meeting ID and select **Attend Meeting**.
8. Verify that you can dial in to the voice meeting by using the "Phone dial-in" and "Meeting ID" values that appear.

   The remaining steps apply only if your system is integrated with Cisco WebEx.
9. Select **Connect** to join the web meeting.
10. Follow the prompts to join the web meeting.
11. If prompted to enter your phone number, then verify that you can join the voice meeting via a dial-out call.
12. Verify that you are signed in as your profile by making sure that your profile name appears in the web meeting room.

Related Topics

- Completing the Installation for the Cisco Unified MeetingPlace Web Server Software with SMA-2S in the Installing the Cisco Unified MeetingPlace Web Server Software in a Segmented Meeting Access (SMA-2S) Configuration module

Disabling SMA-2S

This section describes how to disable SMA-2S, which you need to do before upgrading the Application Server.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.
3. Select **Site**.
4. Select the underlined site name.
5. For the field called "DMZ Web Server", ensure that the value is set to **-none-**.
6. Select **Submit**.