Main page: Cisco Unified MeetingPlace, Release 8.0

Up one level: Configuration

Contents

Overview of Security Tasks

While your company might already have guidelines for securing its computer systems and preventing toll fraud, we also recommend that you perform the tasks listed in Table: Security Recommendations for Cisco Unified MeetingPlace.

Table: Security Recommendations for Cisco Unified MeetingPlace

Recommendation	Where to Find Information
Toll Fraud Prevention	
Restrict dial-out privileges to specific users. **Note:** (Cisco WebEx integration only) Dial-out privileges from the Cisco WebEx site are determined by the guest profile, not by individual user profiles.	• Restricting Dial-Out Privileges for Guest Users • Restricting Dial-Out Privileges for Profiled Users
Monitor dial-out usage.	• Running Capacity Management Reports • Exporting Information about Outgoing Calls* Exporting Meetings
We recommend that you configure Cisco Unified Communications Manager with a Calling Search Space that does the following: • Allows dial-out calls to	• Administration Guide for your release of Cisco Unified Communications Manager at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

meeting participants and the help desk Attendant. • Prevents toll fraud by blocking unwanted dial-out calls, for example, to international or premium-rate phone numbers.	
System Security	
Secure the physical location of the servers. Keep the servers in areas protected by lock or card-key systems to prevent unauthorized access to the systems.	-
Use the Cisco Security Agent on the Application Server.	• Using Cisco Security Agent (CSA) on the Application Server
Use the Secure Socket Layer (SSL) on the Application Server.	• Configuring SSL for the Cisco Unified MeetingPlace Application Server module
Keep the database current. Disable or delete the user profiles of employees who leave the company.	• Locking or Deactivating a User Profile in the Changing the User Status in Cisco Unified MeetingPlace User Profiles module • Deleting a User Profile in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
Change the default passwords for the admin profile.	• Changing the Passwords for the admin Profile in the Changing System Administrator Passwords for Cisco Unified MeetingPlace module

On the router that connects Cisco Unified MeetingPlace to the external network, limit external SSH access to Cisco Unified MeetingPlace to the following: • Safe IP address in your company or organization • Third-party support personnel • Cisco IP addresses: ♦ 128.107.0.0/16 ♦ 198.133.219.0/24 Even if you believe that the SSH sign-in credentials are safe, denial of service attacks can still be launched against your system.	• Documentation for your specific router and software release
Complete as many of these tasks as are appropriate for your user base.	• Configuring Requirements for User Passwords • Limiting the Number of Failed User Sign-in Attempts* Configuring Requirements for Meeting Passwords • Restricting Access to Scheduled Meetings • Restricting Access to Recordings • Restricting the Use of Vanity Meeting IDs
Web Server Security	
Use the Cisco Security Agent on the Web Servers, especially those in the DMZ.	• Working with the Cisco Security Agent (CSA) in the Upgrading to Cisco Unified MeetingPlace Release 8.0 from Cisco Unified MeetingPlace Release 7.0 module
Use McAfee VirusScan Enterprise on the	• *System Requirements for Cisco Unified MeetingPlace* • Documentation provided by McAfee

Web Servers, especially those in the DMZ.	
Enable SSL on the Web Servers.	• How to Configure Secure Sockets Layer for the Web Server in the Configuring Security Features for the Cisco Unified MeetingPlace Web Server module

Related Topics

- Securing the Hardware Media Server module

Using Cisco Security Agent (CSA) on the Application Server

The Cisco Security Agent (CSA) is an application that provides system and data security and allows you to monitor the activities on your system. The CSA is automatically installed on the Application Server with Cisco Unified MeetingPlace and requires no configuration. The red flag at the bottom-right corner of the screen indicates that CSA is running and active on your system.

The CSA consists of a set of rules that govern which users and applications can alter or query critical file systems. It also provides security on ports to minimize unauthorized system sign-ins for malicious purposes. The CSA logs violations of any of the security rules. You can peruse the log periodically to determine what attempted activities were blocked.

Restrictions

Because the CSA application that is included with Cisco Unified MeetingPlace is a standalone version:

- You cannot use the CSA Management Console.
- You cannot manually update the CSA independent of the Application Server. The Application Server software also installs the CSA.

Procedure

1. Sign in to the console.
2. Right-click the red CSA flag in the bottom right.
3. Select **Open Agent Panel**.
4. To change the level of security for your system:
    1. Select **System Security**.
    2. Move the security level slide bar to the new security level.
       Note: We recommend that you keep the security level at medium or high.
5. Select **Status > Messages > View log** to display the logged security events.
6. (Optional) Select **Purge log** to remove the entries that appear on the Status > Messages window.
   Doing this regularly can help you track new events.
   Note: Selecting **Purge log** does not affect the logs under /var/log/csalog.

Limiting the Number of Failed User Sign-in Attempts

You can configure the number of times in a session that an user can fail to sign in to Cisco Unified MeetingPlace before the user profile becomes "locked." Users with locked user profiles cannot sign in.

Restrictions

- The preconfigured system administrator profile cannot be locked.
- Before reaching the maximum number of sign-in attempts, the user can restart the counter for failed sign-in attempts by:
    - Closing the browser and opening a new one to continue the sign-in attempts.
    - Ending the call to Cisco Unified MeetingPlace and making a new call to continue the sign-in attempts.

Procedure

1. Sign in to the Administration Center.
2. Select **System Configuration > Usage Configuration**.
3. Configure the Maximum profile sign-in attempts field. A lower value is more secure than a higher value.
4. Select **Save**.

Related Topics

- Changing the User Status in Cisco Unified MeetingPlace User Profiles module
- Table: Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Configuring Requirements for User Passwords

You can increase the security of your system by:

- Requiring long user passwords
- Requiring users to change their user passwords upon first sign-in
- Requiring users to change their user passwords frequently
- Requiring complex user passwords

Restrictions

- This task does not affect Directory Service users, who are authenticated externally through AXL authentication.

- Long or complex passwords and frequent password changes can frustrate your users. Make sure you align your password requirements with those already in use at your company.

Procedure

1. Sign in to the Administration Center.
2. Select **System Configuration > Usage Configuration**.
3. Configure the following fields, which determine how long passwords must be:
    - ♦ Minimum profile PIN length
    - ♦ Minimum user password length
4. Configure the following fields, which affect when users are required to change their passwords:
    - ♦ Change profile PIN (days)
    - ♦ Change user password (days)
5. Configure the following fields, which determine how complex the user passwords must be:
    - ♦ Password contains characters from at least three classes
    - ♦ No character in the new password repeated more than three times
    - ♦ Password does not repeat or reverse the user ID
    - ♦ Password is not "cisco", "ocsic" or variation of these
6. (Optional) Select **System Configuration > User Profiles**.
    1. Select **Edit** to edit an existing user profile.
    2. Configure these fields to force user password or PIN changes:
        - ◊ Force user password change at next sign-in
        - ◊ Force PIN change at next sign-in
7. Select **Save**.

Related Topics

- Table: Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Table: Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring Cisco Unified MeetingPlace Directory Service module

Configuring Requirements for Meeting Passwords

Meeting passwords prevent uninvited people from attending meetings. You can increase the security of your system by:

- Requiring passwords for meetings scheduled by some or all users
- Requiring long meeting passwords

Before You Begin

Meeting password must be communicated to the meeting invitees in order for them to join the meeting:

- Configure user groups and user profiles to include meeting passwords in email notifications. See the Configuring User Preferences for Email Notifications.

- If not all meeting invitees will receive email notifications, the meeting scheduler or another organizer must manually communicate the meeting password.

Procedure

1. Sign in to the Administration Center.
2. Select **System Configuration > Meeting Configuration**.
3. Configure the Minimum meeting password length field. A higher value is more secure than a lower value.
4. Select **Save**.
5. Select **User Configuration**.
6. Select **User Groups** or **User Profiles**, depending on whether you want to configure a user group or an individual user profile.
7. Select **Edit** or **Add New**, depending on whether you want to configure an existing or a new user group or user profile.
8. Set the Meeting password required to **Yes**.
9. Select **Save**.
10. Repeat Step 5 through Step 9 for all user groups and user profiles for which you want to require meeting passwords.

Related Topics

- Table: Field Reference: Meeting Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Table: Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Restricting Access to Scheduled Meetings

You can restrict uninvited and unprofiled users from attending meetings that are scheduled by some or all users.

Remember, however, that if meeting attendance is restricted to profiled users, unprofiled external users (such as your customers or business partners) and users with locked profiles cannot attend meetings, even if they are invited.

Procedure

1. Sign in to the Administration Center.
2. Select **User Configuration**.
3. Select **User Groups** or **User Profiles**, depending on whether you want to configure a user group or an individual user profile.
4. Select **Edit** or **Add New**, depending on whether you want to configure an existing or a new user group or user profile.

5. Configure the Who can attend field.
6. Select **Save**.

Related Topics

- Table: Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Restricting Access to Recordings

You can restrict unprofiled users from accessing recordings for meetings that are scheduled by some or all users. Remember, however, that if access to recordings is restricted to profiled users, unprofiled external users (such as your customers or business partners) and users with locked profiles cannot access the recordings, even if they were invited to and attended the meetings.

Procedure

1. Sign in to the Administration Center.
2. Select **User Configuration**.
3. Select **User Groups** or **User Profiles**, depending on whether you want to configure a user group or an individual user profile.
4. Select **Edit** or **Add New**, depending on whether you want to configure an existing or a new user group or user profile.
5. Configure the Who can access field.
6. Select **Save**.

Related Topics

- Table: Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Restricting the Use of Vanity Meeting IDs

By default, Cisco Unified MeetingPlace allows the meeting scheduler to request a specific meeting ID, such as one that is easy to remember (12345) or one that spells a word (24726 or CISCO). If, however, an uninvited person knows one of the phone numbers for your Cisco Unified MeetingPlace system, that person can easily guess a popular meeting ID and join a meeting that he is not authorized to attend.

You can prevent unauthorized meeting attendance by disabling the ability to request a vanity meeting ID when scheduling a meeting. Instead, a unique, randomly generated ID is assigned to every scheduled meeting. Users cannot change the assigned meeting IDs.

Procedure

1. Sign in to the Administration Center.
2. Select **System Configuration > Meeting Configuration**.
3. Set the Allow vanity meeting IDs field to **No**.
4. Select **Save**.

Related Topics

- Table: Field Reference: Meeting Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- How to Configure Restricted Meeting ID Patterns in the Configuring Security Features for the Cisco Unified MeetingPlace Web Server module

What To Do Next

You can further prevent unauthorized meeting attendance by:

- Requiring meeting passwords-See the Configuring Requirements for Meeting Passwords.
- Restricting scheduled meeting attendance to profiled users-See the Restricting Access to Scheduled Meetings.

Restricting Dial-Out Privileges for Guest Users

To prevent toll fraud, you can specify that only profiled users who successfully sign in to Cisco Unified MeetingPlace can dial out.

Note: (Cisco WebEx integration only) Completing this task restricts *all* users from dialing out from Cisco WebEx web meetings. Dial-out privileges from Cisco WebEx meetings are determined by the guest profile, not by individual user profiles.

If you disable dial-out privileges in the guest profile, then make sure that you complete the Disabling Dial-Out Calls from the Cisco WebEx Site task in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module.

Procedure

1. Sign in to the Administration Center.
2. Select **User Configuration > User Profiles**.
3. Find the **guest** profile.
4. Select **Edit**.

5. Set the Can dial out (does not apply to Cisco WebEx meetings) field to **No**.
6. Select **Save**.

Related Topics

- Guest Profile in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
- Table: Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Restricting Dial-Out Privileges for Profiled Users
- Limiting the Number of Attempted Dial-Out Calls From Voice Meetings
- Enabling Dial-Out Calls from the Cisco WebEx Web Meeting Room in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module

Restricting Dial-Out Privileges for Profiled Users

To prevent toll fraud, you can restrict dial-out privileges to specific user groups and user profiles.

Procedure

1. Sign in to the Administration Center.
2. Select **User Configuration**.
3. To restrict dial-out privileges for specific user groups, select **User Groups**. To restrict dial-out privileges for specific user profiles, select **User Profiles**.
4. Select a user group or user profile and select **Edit** in the same row.
5. Set Can dial out (does not apply to Cisco WebEx meetings) to **No**.
6. Select **Save**.

Related Topics

- Table: Navigation Reference: User Groups Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Table: Navigation Reference: User Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Restricting Dial-Out Privileges for Guest Users
- Limiting the Number of Attempted Dial-Out Calls From Voice Meetings

Limiting the Number of Attempted Dial-Out Calls From Voice Meetings

To prevent toll fraud, you can specify the maximum number of dial-out calls that each user can try to make from within a meeting.

Restriction

This procedure affects only the dial-out calls that the user attempts by pressing #31 from the telephone user interface (TUI). You cannot limit the number of dial-out calls that are attempted from the web meeting room.

Procedure

1. Sign in to the Administration Center.
2. Select **User Configuration**.
3. To restrict dial-out privileges for specific user groups, select **User Groups**. To restrict dial-out privileges for specific user profiles, select **User Profiles**.
4. Select a user group or user profile and select **Edit** in the same row.
5. Configure the Maximum TUI dial-out attempts per meeting field.
   We recommend restricting the dial-out attempts to as low a number as possible while accommodating the dial-out needs of your users.
6. Select **Save**.

Related Topics

- Table: Navigation Reference: User Groups Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Table: Navigation Reference: User Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Restricting Dial-Out Privileges for Guest Users
- Restricting Dial-Out Privileges for Profiled Users