Securing the Cisco Unified MeetingPlace System

Release 7.1
Revised: April 6, 2011 12:14 pm

Overview of Security Tasks

While your company may already have guidelines for securing its computer systems and preventing toll fraud, we also recommend that you perform the tasks listed in Table 1.

Table 1 Security Recommendations for Cisco Unified MeetingPlace

Recommendation	Where to Find Information
Toll Fraud Prevention	
Restrict dial-out privileges to specific users.	• Restricting Dial-Out Privileges for Guest Users, page 9 • Restricting Dial-Out Privileges for Profiled Users, page 10

Table 1 Security Recommendations for Cisco Unified MeetingPlace (continued)

Recommendation	Where to Find Information
Monitor dial-out usage.	• Running Capacity Management Reports, page 11 • Exporting Information about Dial-Out Calls, page 12 • Exporting Meetings, page 6
We recommend that you configure Cisco Unified Communications Manager with a Calling Search Space that does the following: • Allows dial-out calls to meeting participants and the help desk Attendant. • Prevents toll fraud by blocking unwanted dial-out calls, for example, to international or premium-rate telephone numbers.	• 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
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, page 3 • Upgrading Cisco Security Agent (CSA) on the Application Server, page 4
Use the Secure Socket Layer (SSL) on the Application Server.	• Configuring SSL for the Cisco Unified MeetingPlace Application Server module
Keep the database current. Deactivate 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 login credentials are safe, denial of service attacks may still be launched against your system.	• Documentation for your specific router and software release

Table 1 Security Recommendations for Cisco Unified MeetingPlace (continued)

Recommendation	Where to Find Information
Complete as many of these tasks as are appropriate for your user base.	• Configuring Requirements for User Passwords, page 6 • Limiting the Number of Failed User Login Attempts, page 5 • Configuring Requirements for Meeting Passwords, page 7 • Restricting Access to Scheduled Meetings, page 8 • Restricting Access to Recordings and Attachments, page 8 • Restricting the Use of Vanity Meeting IDs, page 9
Web Server Security	
Use the Cisco Security Agent on the Web Servers, especially those in the DMZ.	• Installing the Cisco Security Agent in the How to Install the Cisco Unified MeetingPlace Web Conferencing Server module of the *Installation, Upgrade, and Migration Guide for Cisco Unified MeetingPlace*
Use McAfee VirusScan Enterprise on the Web Servers, especially those in the DMZ.	• *System Requirements and Compatibility Matrix for Cisco Unified MeetingPlace* • Documentation provided by McAfee
Enable SSL on the Web Servers.	• How to Configure Secure Sockets Layer in the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features 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 logins for malicious purposes. The CSA logs violations of any of the security rules. You may 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.
- If a newer version of CSA comes out, you must manually upgrade CSA on the Application Server. See the "Upgrading Cisco Security Agent (CSA) on the Application Server" section on page 4.

Procedure

Step 1 Log in to the console.

Step 2 Right-click the red CSA flag in the bottom right.

Step 3 Choose **Open Agent Panel**.

Step 4 To change the level of security for your system:

a. Select **System Security**.

b. Move the security level slide bar to the new security level.

Note We recommend that you keep the security level at medium or high.

Step 5 Select **Status > Messages > View log** to display the logged security events.

Step 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.

Related Topics

- Upgrading Cisco Security Agent (CSA) on the Application Server, page 4
- "Installing the Cisco Security Agent" in the Installing the Cisco Unified MeetingPlace Web Conferencing Server chapter of the *Installation, Upgrade, and Migration Guide for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html

Upgrading Cisco Security Agent (CSA) on the Application Server

Before You Begin

Read the *System Requirements for Cisco Unified MeetingPlace* Release 7.1.

Procedure

Step 1 Go to Cisco.com and find the Cisco Security Agent upgrade file.

The CSA is distributed as an RPM file on a CD or as a file download. The filename will be similar to CSA_5.1.0.95.

Step 2 Save the file to a convenient location.

Step 3 From the console, go to the Cisco Unified MeetingPlace operating system login page.

Step 4 Log in as the root user.

Step 5 Right-click the desktop and select **New Terminal**.

Step 6 Navigate to the directory where you saved the CSA upgrade file.

Step 7 Enter **rpm -e cisco-CSA_package** to uninstall the previous CSA version.

Step 8 Enter **rpm -Uvh <CSA-upgrade-filename>** to execute the program.

Example: rpm -Uvh CSA_5.1.0.95

Step 9 Enter **reboot**.

Related Topics

- Logging in to the CLI Using the Console in the Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- Using Cisco Security Agent (CSA) on the Application Server, page 3
- "Installing the Cisco Security Agent" in the Installing the Cisco Unified MeetingPlace Web Conferencing Server chapter of the *Installation, Upgrade, and Migration Guide for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html

Limiting the Number of Failed User Login Attempts

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

Restrictions

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

Procedure

Step 1 Log in to the Administration Center.

Step 2 Select **System Configuration > Usage Configuration**.

Step 3 Configure the Maximum profile login attempts field. A lower value is more secure than a higher value.

Step 4 Select **Save**.

Related Topics

- Changing the User Status in Cisco Unified MeetingPlace User Profiles module
- 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 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 may frustrate your users. Make sure you align your password requirements with those already in use at your company.

Procedure

Step 1 Log in to the Administration Center.

Step 2 Select **System Configuration > Usage Configuration**.

Step 3 Configure the following fields, which determine how long passwords must be:

- Minimum profile password length
- Minimum user password length

Step 4 Configure the following fields, which affect when users are required to change their passwords:

- Change profile password (days)
- Change user password (days)

Step 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 name
- Password is not "cisco", "ocsic" or variation of these

Step 6 Select **Save**.

Related Topics

- Field Reference: Usage Configuration 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 e-mail notifications. See the "Configuring User Preferences for E-Mail Notifications" section on page 3.
- If not all meeting invitees will receive e-mail notifications, the meeting scheduler or another organizer must manually communicate the meeting password.

Procedure

Step 1 Log in to the Administration Center.

Step 2 Select **System Configuration** > **Meeting Configuration**.

Step 3 Configure the Minimum meeting password length field. A higher value is more secure than a lower value.

Step 4 Select **Save**.

Step 5 Select **User Configuration**.

Step 6 Select **User Groups** or **User Profiles**, depending on whether you want to configure a user group or an individual user profile.

Step 7 Select **Edit** or **Add New**, depending on whether you want to configure an existing or a new user group or user profile.

Step 8 Set the Meeting password required to **Yes**.

Step 9 Select **Save**.

Step 10 Repeat Step 5 through Step 9 for all user groups and user profiles for which you want to require meeting passwords.

Related Topics

- Field Reference: Meeting Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- 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, then unprofiled external users (such as your customers or business partners) and users with locked profiles cannot attend meetings, even if they are invited.

Procedure

Step 1 Log in to the Administration Center.

Step 2 Select **User Configuration**.

Step 3 Select **User Groups** or **User Profiles**, depending on whether you want to configure a user group or an individual user profile.

Step 4 Select **Edit** or **Add New**, depending on whether you want to configure an existing or a new user group or user profile.

Step 5 Configure the Who can attend field.

Step 6 Select **Save**.

Related Topics

- 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 and Attachments

You can restrict unprofiled users from accessing recordings and attachments for meetings that are scheduled by some or all users. Remember, however, that if access to recordings is restricted to profiled users, then 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

Step 1 Log in to the Administration Center.

Step 2 Select **User Configuration**.

Step 3 Select **User Groups** or **User Profiles**, depending on whether you want to configure a user group or an individual user profile.

Step 4 Select **Edit** or **Add New**, depending on whether you want to configure an existing or a new user group or user profile.

Step 5 Configure the Who can access field.

Step 6 Select **Save**.

Related Topics

- 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

Step 1 Log in to the Administration Center.

Step 2 Select **System Configuration > Meeting Configuration**.

Step 3 Set the Allow vanity meeting IDs field to **No**.

Step 4 Select **Save**.

Related Topics

- Field Reference: Meeting Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module

What To Do Next

You can further prevent unauthorized meeting attendance by:

- Requiring meeting passwords—See the "Configuring Requirements for Meeting Passwords" section on page 7.
- Restricting scheduled meeting attendance to profiled users—See the "Restricting Access to Scheduled Meetings" section on page 8.

Restricting Dial-Out Privileges for Guest Users

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

Procedure

Step 1 Log in to the Administration Center.

Step 2 Select **User Configuration > User Profiles**.

Step 3 Find the **guest** profile.

Step 4 Select **Edit**.

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

Step 6 Select **Save**.

Related Topics

- Guest Profile in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
- 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, page 10
- Limiting the Number of Attempted Dial-Out Calls From Voice Meetings, page 11

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

Step 1 Log in to the Administration Center.

Step 2 Select **User Configuration**.

Step 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**.

Step 4 Select a user group or user profile and select **Edit** in the same row.

Step 5 To restrict dial-out privileges, configure the following fields:

- Can dial out (does not apply to Cisco WebEx meetings)—Set to **No**.
- Ask for profile password—Set to **Yes**.

Step 6 Select **Save**.

Related Topics

- Navigation Reference: User Groups Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Navigation Reference: User Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Restricting Dial-Out Privileges for Guest Users, page 9
- Limiting the Number of Attempted Dial-Out Calls From Voice Meetings, page 11

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

Step 1 Log in to the Administration Center.

Step 2 Select **User Configuration**.

Step 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**.

Step 4 Select a user group or user profile and select **Edit** in the same row.

Step 5 Configure the Maximum TUI outdial 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.

Step 6 Select **Save**.

Related Topics

- Navigation Reference: User Groups Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Navigation Reference: User Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Restricting Dial-Out Privileges for Guest Users, page 9
- Restricting Dial-Out Privileges for Profiled Users, page 10