Configuring Security Features for Cisco Unified MeetingPlace Express

Revised: May 1, 2006, OL-6664-04

The following topics describe ways to increase the security of your Cisco Unified MeetingPlace Express system:

- Configuring User Password Requirements, page 9-1
- Limiting the Number of Failed User Login Attempts, page 9-2
- Configuring Requirements for Meeting Passwords, page 9-3
- Restricting Access to Scheduled Meetings and Recordings, page 9-4
- Restricting the Use of Vanity Meeting IDs, page 9-5
- Restricting Third Parties from Starting Reservationless Meetings, page 9-6
- About Toll Fraud Prevention, page 9-6
- Changing the Admin Passwords, page 1-2

Configuring User Password Requirements

You can increase the security of your Cisco Unified MeetingPlace Express system by doing the following:

- Requiring longer user passwords
- Requiring users to change their passwords more frequently

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page:

a. Click **System Configuration**.

b. Click **Usage Configuration**.

Step 4 In the Usage Configuration page, configure the following fields:

- Minimum profile password length, page B-189—A higher value is more secure than a lower value.
- Change profile password (days), page B-189—A lower value is more secure than a higher value.
- Minimum user password length, page B-189—A higher value is more secure than a lower value.
- Change user password (days), page B-189—A lower value is more secure than a higher value.

Step 5 Click **Save**.

Tip

Remember that long passwords and frequent password changes may frustrate your users. Align your password requirements with those already in use at your company.

Related Topics

- Configuring Security Features for Cisco Unified MeetingPlace Express, page 9-1
- About This Page: Usage Configuration, page B-188

Limiting the Number of Failed User Login Attempts

This topic describes how to configure the number of times in a session that a user can fail to log in to Cisco Unified MeetingPlace Express before the user profile becomes "locked." Users with locked user profiles cannot log in to Cisco Unified MeetingPlace Express. For more information about locked profiles, see the "About the Active, Inactive, and Locked States of User Profiles" section on page 6-31.

Before You Begin

- The preconfigured admin user profile cannot be locked.
- Before reaching the maximum number of login attempts, the user may restart the counter for failed login attempts by taking one of the following actions:
  - Close the browser and open a new one to continue the login attempts.
  - End the call to Cisco Unified MeetingPlace Express and begin a new call to continue the login attempts.
- Calls to the attendant are not supported if you use a SIP trunk to integrate Cisco Unified MeetingPlace Express with Cisco Unified CallManager Release 4.x. For more information about this restriction, see the Cisco Unified CallManager Restrictions for Integration in a SIP Environment in the "About Integration in a SIP Environment" section on page 5-39.

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page:

a. Click **System Configuration**.

b. Click **Usage Configuration**.

Step 4 In the Usage Configuration page, configure the following field:

- Maximum profile login attempts, page B-190—A lower value is more secure than a higher value.

Step 5 Click **Save**.

Related Topics

- Configuring Security Features for Cisco Unified MeetingPlace Express, page 9-1
- About the Active, Inactive, and Locked States of User Profiles, page 6-31
- About This Page: Usage Configuration, page B-188

Configuring Requirements for Meeting Passwords

You can increase the security of your Cisco Unified MeetingPlace Express system by doing the following:

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

Meeting passwords prevent uninvited people from attending meetings.

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page, click **Meeting Configuration**.

Step 4 In the Meeting Configuration page, configure the following field:

- Minimum meeting password length, page B-124—A higher value is more secure than a lower value.

Step 5 Click **Save**.

Step 6 On the left side of the page, click **User Configuration**.

Step 7 Take one of the following actions:

- To configure a user group, click **User Group Management**.
- To configure an individual user profile, click **User Profile Management**.

Step 8 Take one of the following actions:

- To configure an existing user group or user profile, click **Edit**.
- To configure a new user group or user profile, click **Add New**. Configure the required fields, which are marked with an asterisk.

Step 9 Configure one of the following fields:

- Password required, page B-12 (user group)—Select **Yes**.
- Password required, page B-24 (user profile)—Select **Yes**.

Step 10 Click **Save**.

Step 11 Repeat Step 6 through Step 10 for all user groups and user profiles for which you want to require meeting passwords.

Tips

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

- Configure user groups and user profiles to include passwords in e-mail notifications. See the "Configuring E-Mail Notification Settings for a User Group" section on page 12-3.
- If not all meeting invitees will receive e-mail notifications, then the meeting scheduler or another organizer must manually communicate the meeting password.

Related Topics

- Configuring Security Features for Cisco Unified MeetingPlace Express, page 9-1
- About This Page: Meeting Configuration, page B-121
- About This Page: Add User Group, page B-9
- About This Page: Add User Profile, page B-16

Restricting Access to Scheduled Meetings and Recordings

This topic describes how to restrict unprofiled users from taking the following actions:

- Attend meetings that are scheduled by some or all users.
- Listen to meetings recorded by some or all users.

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page, click **User Configuration**.

Step 4 Take one of the following actions:

- To configure a user group, click **User Group Management**.
- To configure an individual user profile, click **User Profile Management**.

Step 5 Take one of the following actions:

- To configure an existing user group or user profile, click **Edit**.
- To configure a new user group or user profile, click **Add New**. Configure the required fields, which are marked with an asterisk.

Step 6 To restrict meeting attendance *and* access to meeting recordings to profiled users, configure one of the following fields to Users with Cisco Unified MeetingPlace Express profiles only:

- Who can attend, page B-12 (user group)
- Who can attend, page B-24 (user profile)

Step 7 Click **Save**.

Step 8 Repeat Step 3 through Step 7 for all user groups and user profiles for which you want to restrict meeting access to profiled users.

Tips

- Remember 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.
- Similarly, if access to meeting recordings is restricted to profiled users, then unprofiled external users (such as your customers or business partners) and users with locked profiles cannot access these meeting recordings.

Related Topics

- Configuring Security Features for Cisco Unified MeetingPlace Express, page 9-1
- About This Page: Add User Group, page B-9
- About This Page: Add User Profile, page B-16

Restricting the Use of Vanity Meeting IDs

By default, Cisco Unified MeetingPlace Express 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 the phone number of your Cisco Unified MeetingPlace Express server, then that person can easily guess a popular meeting ID and join a meeting that he is not authorized to attend.

This topic describes how to 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 Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page, click **Meeting Configuration**.

Step 4 In the Meeting Configuration page, configure the following field:

- Allow vanity meeting IDs, page B-125—Select **No**.

Step 5 Click **Save**.

Tips

You can also prevent unauthorized meeting attendance in the following ways:

- Requiring meeting passwords—See the "Configuring Requirements for Meeting Passwords" section on page 9-3.
- Restricting scheduled meeting attendance to profiled users—See the "Restricting Access to Scheduled Meetings and Recordings" section on page 9-4.

Related Topics

- Configuring Security Features for Cisco Unified MeetingPlace Express, page 9-1
- About This Page: Meeting Configuration, page B-121

Restricting Third Parties from Starting Reservationless Meetings

This topic describes how to configure the system so that only the meeting owner may start a reservationless meeting. For more information about reservationless meetings, see the "About Reservationless Meetings" section on page 4-6.

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page:

a. Click **System Configuration**.

b. Click **Meeting Configuration**.

Step 4 In the Meeting Configuration page, configure the following field:

- Reservationless: Allow 3rd Party Initiate?, page B-125—Select **No**.

Step 5 Click **Save**.

Related Topics

- Configuring Security Features for Cisco Unified MeetingPlace Express, page 9-1
- About the Active, Inactive, and Locked States of User Profiles, page 6-31
- About This Page: Usage Configuration, page B-188

About Toll Fraud Prevention

Cisco Unified MeetingPlace Express enables you to monitor and prevent toll fraud occurrences by performing the following tasks:

- Restricting dial-out privileges to specific user groups or user profiles. See the following topics:
  - Restricting Dial-Out Privileges for Guest Users, page 9-7
  - Restricting Dial-Out Privileges for Profiled Users, page 9-7.
- Monitoring dial-out usage. See the following topics:
  - Running a Report about Port Utilization, page 8-11
  - Exporting Information about Outgoing Calls, page 8-14
  - Exporting Information about Meetings, page 8-6

Related Topics

- Configuring Security Features for Cisco Unified MeetingPlace Express, page 9-1

Restricting Dial-Out Privileges for Guest Users

This topic describes how to restrict guests from dialing out. By completing this task, only profiled users who successfully log in to Cisco Unified MeetingPlace Express can dial out. This restriction can reduce the potential for toll fraud.

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 On the left side of the page:

a. Click **System Configuration**.

b. Click **Usage Configuration**.

Step 4 In the Usage Configuration page, set the Allow guest outdials field to **No**.

Step 5 Click **Save**.

Tips

To further restrict dial-out privileges on your system, proceed to the "Restricting Dial-Out Privileges for Profiled Users" section on page 9-7.

Related Topics

- About Dial-Out Features and Voice Prompt Languages, page 6-18
- About Toll Fraud Prevention, page 9-6
- Restricting Dial-Out Privileges for Profiled Users, page 9-7
- Exporting Information about Outgoing Calls, page 8-14
- About This Page: User Group Management, page B-196
- About This Page: User Profile Management, page B-198

Restricting Dial-Out Privileges for Profiled Users

This topic describes how to restrict dial-out privileges to specific user groups and user profiles. Restricting dial-out privileges reduces the potential for toll fraud.

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express.

Step 2 Click **Administration** at the top of the page.

Step 3 Click **User Configuration** on the left side of the page.

Step 4 To restrict dial-out privileges for specific user groups, complete these steps:

a. Click **User Group Management**.

b. In the User Group Management page, select a user group and click **Edit** in the same row. The Edit User Groups Details page appears.

c. To restrict dial-out privileges, configure the following fields, which are described in the "About This Page: Add User Group" section on page B-9:

- Can call out of meetings—Set to **No**.
- Ask for profile password—Set to **Yes**.

d. Click **Save**.

e. Repeat Step 4 for all user groups whose dial-out privileges you want to restrict.

Step 5 To restrict dial-out privileges for specific user profiles, complete these steps:

a. Click **User Profile Management**.

b. In the User Profile Management page, select a user profile and click **Edit** in the same row. The Edit user profiles details page appears.

c. To restrict dial-out privileges, configure the following fields, which are described in the "About This Page: Add User Profile" section on page B-16:

- Can call out of meetings?—Set to **No**.
- Ask for profile password?—Set to **Yes**.

d. Click **Save**.

e. Repeat Step 5 for all user profiles whose dial-out privileges you want to restrict.

Related Topics

- About Dial-Out Features and Voice Prompt Languages, page 6-18
- About Toll Fraud Prevention, page 9-6
- Restricting Dial-Out Privileges for Guest Users, page 9-7
- Exporting Information about Outgoing Calls, page 8-14
- About This Page: User Group Management, page B-196
- About This Page: User Profile Management, page B-198