Contents

Enabling Password Complexity for the mpxadmin User

Note: This section only applies to Release 2.1.x.

You can increase the security of your Cisco Unified MeetingPlace Express system by enabling password complexity for the mpxadmin user. Complex passwords have the following characteristics:

- Must be 14 characters or longer
- Must contain at least two lowercase characters
- Must contain at least two uppercase characters
- Must contain at least two digits
- Must contain at least two special characters
- Must be changed at least every 60 days

Notes:

- When the mpxadmin user logs in after the mpxadmin password has expired, the system prompts the mpxadmin user to change it.

- If the mpxadmin password has expired, the application will not come up. You can restart the system, but until you change the mpxadmin password, the application services will not start properly.

Procedure

1. Log in to the Cisco Unified MeetingPlace Express operating system as the **mpxadmin** user.
2. At the password prompt, enter the mpxadmin password.
3. Right-click on the desktop.
4. From the menu, select **New Terminal**. This brings up a terminal session.
5. Enable password complexity for the mpxadmin user by entering the following:
   $MP_OS_HOME/enable_complex_passwd.sh
6. Disable password complexity for the mpxadmin user by entering the following:
   $MP_OS_HOME/disable_complex_passwd.sh

Configuring User Password Requirements

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

- Requiring long user passwords
- Requiring users to change their passwords frequently

Tip

- Long passwords and frequent password changes may frustrate your users. Align your password requirements with those already in use at your company.

Procedure

1. Log in to Cisco Unified MeetingPlace Express and click **Administration**.
2. Click **System Configuration > Usage Configuration**.
3. Configure the following fields:
   - ♦ Minimum profile password length-A higher value is more secure than a lower value.
   - ♦ Change profile password (days)-A lower value is more secure than a higher value.
   - ♦ Minimum user password length-A higher value is more secure than a lower value.
   - ♦ Change user password (days)-A lower value is more secure than a higher value.
4. Click **Save**.

Related Topics

- Field Reference: Usage Configuration

Limiting the Number of Failed User Login Attempts

This topic describes how to configure the number of times in a session that an end 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.

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.

Restriction

- The preconfigured system administrator profile cannot be locked.

Procedure

1. Log in to Cisco Unified MeetingPlace Express and click **Administration**.
2. Click **System Configuration > Usage Configuration**.
3. Configure the Maximum profile login attempts field. A lower value is more secure than a higher value.
4. Click **Save**.

Related Topics

- How to Change the State of a User Profile
- Field Reference: Usage Configuration

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 long meeting passwords

Meeting passwords prevent uninvited people from attending meetings. The meeting passwords are recognised as a numeric form, that is, even if you have set an alphabetical password for a scheduled meeting, each character of the password will be recorded as a numeric digit based on the telephone keypad. For example, 'turnaround' will be recorded as '8876276863'.

Procedure

1. Log in to Cisco Unified MeetingPlace Express and click **Administration**.
2. Click **System Configuration > Meeting Configuration**.
3. Configure the Minimum meeting password length field. A higher value is more secure than a lower value.
4. Click **Save**.
5. Click **System Configuration > User Configuration**.
6. To configure a user group, click **User Group Management**. To configure an individual user profile, click **User Profile Management**.
7. To configure an existing user group or user profile, click **Edit**. To configure a new user group or user profile, click **Add New**.
8. Set the Password required to **Yes**.
9. Click **Save**.
10. Repeat Step 5 through Step 9 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.
- If not all meeting invitees will receive e-mail notifications, the meeting scheduler or another organizer must manually communicate the meeting password.

Related Topics

- Field Reference: Meeting Configuration
- Field Reference: Add User Group
- Field Reference: Add User Profile

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

1. Log in to Cisco Unified MeetingPlace Express and click **Administration**.
2. Click **System Configuration > User Configuration**.
3. To configure a user group, click **User Group Management**. To configure an individual user profile, click **User Profile Management**.

4. To configure an existing user group or user profile, click **Edit**. To configure a new user group or user profile, click **Add New**.
5. To restrict meeting attendance *and* access to meeting recordings to profiled users, set the Who can attend field to "Users with Cisco Unified MeetingPlace Express profiles only":
6. Click **Save**.
7. Repeat Step 2 through Step 6 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

- Field Reference: Add User Group
- Field Reference: Add User Profile

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, that person can easily guess a popular meeting ID and join a meeting that he is not authorized to attend.

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

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

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

1. Log in to Cisco Unified MeetingPlace Express and click **Administration**.
2. Click **System Configuration > Meeting Configuration**.
3. Set the Allow vanity meeting IDs field to **No**.

4. Click **Save**.

Related Topics

- Field Reference: Meeting Configuration

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.

Procedure

1. Log in to Cisco Unified MeetingPlace Express and click **Administration**.
2. Click **System Configuration > Meeting Configuration**.
3. Set the Reservationless: Allow 3rd party initiate field to **No**.
4. Click **Save**.

Related Topics

- Enabling Users to Schedule Reservationless Meetings
- Field Reference: Meeting Configuration

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

1. Log in to Cisco Unified MeetingPlace Express and click **Administration**.
2. Click **System Configuration > Usage Configuration**.
3. Set the Allow guest outdials field to **No**.
4. Click **Save**.

Related Topics

- Restricting Dial-Out Privileges for Profiled Users
- Field Reference: Usage Configuration

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

1. Log in to Cisco Unified MeetingPlace Express and click **Administration**.
2. Click **User Configuration**.
3. To restrict dial-out privileges for specific user groups, click **User Group Management**. To restrict dial-out privileges for specific user profiles, click **User Profile Management**.
4. Select a user group or user profile and click **Edit** in the same row.
5. To restrict dial-out privileges, configure the following fields:
    - Can call out from meetings-Set to **No**.
    - Ask for profile password-Set to **Yes**.
6. Click **Save**.

Related Topics

- Restricting Dial-Out Privileges for Guest Users
- Navigating the User Group Management Page
- Navigating the User Profile Management Page