The security of your Cisco Unified MeetingPlace system includes physical security, software security, and toll-fraud prevention. Your company may already have guidelines for protecting the security of its computer systems.

Contents

Securing the Location

Securing the location of your system prevents unauthorized access to the system technician console port.

Caution! Keep the system in an area protected by a lock or a card-key system.

Securing User Profiles

To prevent unauthorized users from accessing Cisco Unified MeetingPlace over the phone or from a computer, use the security measures described in Table: Methods for Securing User Profiles.

Table: Methods for Securing User Profiles

Action	Description
Use password protection	Cisco Unified MeetingPlace requires passwords for access from a phone or computer. User passwords permit access from a computer, and profile passwords permit access over a phone.

	To ensure effective use of profile passwords, administer the minimum password length and password change parameters in the Configure tab to define password information, including the following: • Min profile pwd length (minimum profile password length for phone access) • Change profile pwd (how often users must change their profile passwords) • Min user pwd length (minimum workstation access password length) • Change user pwd (how often users must change their workstation access passwords) • Min meeting pwd length (minimum length for a meeting password) **Note:** We recommend that you require users to change passwords according to your company's policies for similar systems.
Use hacker lockout	Cisco Unified MeetingPlace offers a "hacker lockout" feature, which deactivates any user profile after a number of consecutive, unsuccessful login attempts. You define the number of attempts. To do so: 1. In the MeetingTime Configure tab, select the **Usage Parameters** topic. 2. Enter the maximum number of attempts to access the user profiles (**Max profile login attempts** or **Max profile login/mtg password attempts**, depending on your release version). After users reach the maximum number of retries by phone, the profile is locked. Further attempts to log in result in a "Profile is invalid" message, the caller is transferred to the attendant, and a minor alarm is generated. **Note for Cisco Unified MeetingPlace Release 6.0, Maintenance Release 3:** The Max profile login attempts parameter is also used to define the number of consecutive, unsuccessful attempts to start a reservationless meeting that the system allows. If the user exceeds this number of attempts to start a reservationless meeting using a profile number and password, the system will lock out the profile. To unlock a user profile: 1. In the MeetingPlace System tab, select the **View Locked Profiles** action. 2. Change the User Active? setting in the profile to **Yes** . (Until you do, this profile cannot be used.) For more information on resetting locked profiles, see the Problem: User Cannot Log In. Users who exceed the limit of password attempts by computer in MeetingTime are exited from the application. Users can then double-click the MeetingTime icon and try again. (Security is less stringent from the computer than from the phone because outdialing is not an issue.) **Note:** This feature can expose the server to a denial of service attack: a hacker simply goes through the list of profiles and locks them all by entering bad passwords, which renders the system unusable until the system administrator unlocks the accounts. Hackers

	can (and will) avoid the lockout by trying different profile numbers with the same commonly used password rather than the other way around. Consequently, many secure installations do not employ this feature. Cisco recommends that you weigh the costs of possibly making it easier for a hacker to break into an account versus the costs of managing locked accounts and running the risk of critical accounts being locked in an emergency.
Keep the database current	You can also ensure user profile security by maintaining an up-to-date user database. For example, delete or deactivate user profiles of employees who leave the company. For details on removing profiles from the system, see the About Maintaining the User Database.
Use Cisco Unified MeetingPlace SNMP agent	The Cisco Unified MeetingPlace Simple Network Management Protocol (SNMP) agent comes preconfigured with communities labeled MeetingPlace-public and MeetingPlace-private. To prevent unauthorized queries, Cisco recommends changing these community names to names chosen by the customer. For details on changing community names, see the Setting Up Community Information. The Cisco Unified MeetingPlace SNMP agent is based on SNMPv1 code, which has security vulnerabilities known to hackers. Cisco recommends blocking the SNMP port using a firewall. If the Cisco Unified MeetingPlace Audio Server is located on the network so that a firewall cannot protect the SNMP port, we recommend disabling SNMP queries. This can be done without disabling trap generation.

Securing Meetings

All meetings are protected by meeting ID numbers. For each scheduled meeting, you can determine whether the meeting requires both a password and a meeting ID.

If you do not want end users to see listings for meetings to which they have not been invited, the Display Meeting to Everyone? attribute must be set to No when scheduling a meeting. If this attribute is set to *Yes* , any profile user can view information about this meeting from the Browse Meetings link in Cisco Unified MeetingPlace Web Conferencing and from the MeetingTime interface.

Table: Methods for Securing Meetings describes ways to secure meetings.

Table: Methods for Securing Meetings

Action	Description
Use meeting passwords	Meeting passwords provide an additional level of security to the meeting. By using the Usage Parameters topic in the Configure tab, you can define the minimum length for a meeting password (Min meeting pwd length).
Maintenance Release 3 and later:	Set the Max profile login/mtg password attempts parameter (in Usage Parameters in MeetingTime)

Limit the number of attempts to join a password-protected meeting	
Restrict meeting attendance	The Who Can Attend attribute allows meeting schedulers to restrict meeting attendance to those users with Cisco Unified MeetingPlace profiles or to profile users who are explicitly invited to meetings. Restricting meeting attendance prevents guest users from joining the meeting.
Secure meetings in session	During a meeting, users can access the in-session meeting features and use the following admittance options to control who can enter the meeting: • **#21** takes roll call of current participants • **#41** locks meeting to prevent additional parties from joining the meeting without permission • **#42** admits unannounced participant to meeting • **#43** drops last participant who enters the meeting
Restrict access to meeting records	You can restrict users from recording meetings from the User Profile and User Groups topics in the Configure tab. When scheduling meetings you can determine whether access to recordings of certain meetings are restricted to specific users or require a password.
Restrict use of vanity meeting IDs	When users schedule meetings, by default they can assign *vanity* (custom or common) meeting IDs, such as 1234. Although vanity meeting IDs are easier for meeting participants to remember and identify, you may want to restrict their use. Doing so adds a level of security and prevents unauthorized users or hackers from easily guessing the ID and gaining access to the meeting. To restrict vanity IDs: 1. In the Configure tab, select **System Parameters** . 2. For the **Allow Vanity Mtg IDs** field, choose **No** . The system assigns a unique, randomly generated ID (which users cannot change) to every meeting scheduled from then on. When users are allowed to assign vanity IDs, you can add a level of security by restricting groups or individual users from assigning vanity IDs to meetings that are scheduled by phone. To do so: 1. In the Configure tab, select **User Groups or User Profiles** . 2. For the Can Chg Mtg ID Via Phone field, choose **No** . User profiles inherit the group setting, but system administrators can change the setting for individual users. **Note:** To protect meeting IDs that can be hacked easily (such as 1234 or ABCD), create zero-port continuous meetings and assign those meeting IDs. Limit those meetings to invitees only, and do not invite other people. (For more information about continuous meetings, see the About Continuous Meetings.)

Preventing Toll Fraud

Although recent court decisions and Federal Communications Commission (FCC) regulations stipulate that toll fraud is the customer's responsibility and not the responsibility of the equipment vendors, Cisco Unified MeetingPlace provides several ways to prevent unauthorized use. Because Cisco Unified MeetingPlace is a

powerful telecommunications system allowing calls in and out, it is important to take measures to prevent unauthorized access to your system, as shown in Table: Methods for Preventing Toll Fraud.

Table: Methods for Preventing Toll Fraud

Action	Description
Restrict outdialing privileges	The first level of protection against toll fraud is the user profile, which determines a user's outdial privileges and whether they can schedule meetings that allow guests to attend over the Web. You can restrict outdialing privileges to specific user groups, such as sales and marketing, or to specific user profiles, such as Jones and Smith. In the most extreme case, you can choose to disable impromptu outdialing for all users, virtually eliminating the potential for toll fraud. To ensure that only registered users can outdial from within meetings: 1. In the Configure tab, select the **User Profiles** topic. 2. For the Can Call Out From Mtgs? attribute, make sure it is set to *No* in the guest profile. 3. Repeat steps 1 and 2 for the **User Groups** topic. 4. To restrict the number of outdials a particular user or guest can make from within each meeting (by pressing **#3**), set the Max Outdials Per Mtg attribute to a low number. In addition, if you do not want the system to outdial to guests when they click the **Join Voice Conference** button from the Web, make sure the Can Allow Guest Outdial in Mtgs attribute is set to No in all user profiles. For more information on this attribute, see the About User Profiles. **Note:** Setting the user profile attribute Can Call Out From Meetings to *No* does not prevent the user from scheduling a meeting with the Outdial Invitees on First Call attribute set to Yes.
Limit near-term meetings	You can limit the number of near-term meetings (meetings scheduled to occur within six hours of the scheduling time) by setting the near-term limit for the User Groups and User Profiles topics.
Define system-wide restrictions	The next level of security consists of the system outdialing translation tables. The translation tables define which phone numbers the Cisco Unified MeetingPlace system can call. You can configure the system with up to 16 different tables to provide unique capabilities for different user communities on the system. You can also define tables through a PBX. Remember the following information: • Be specific about who can and cannot outdial. In the Port Groups and Ports topics in the Configure tab, you can set which ports can handle outgoing calls. You can also set users' outdial privileges in their individual user profiles, or restrict the

	number of outdials users can make during a meeting. • Define an internal dialing table to restrict specific long distance calls. A Cisco Network Consulting Engineer (NCE) can assist you in setting up a dialing table. • Through a PBX, use blocking tables to block outdial to certain area codes. • Check with your long distance vendor to monitor the use of outgoing lines for unusual outgoing calls.
Monitor usage through reports	You can easily review outdialing usage to look for toll fraud patterns. Cisco Unified MeetingPlace provides both a standard outbound dialing report and the capability to export raw data to third party software programs. Use the MeetingTime Outbound Dialing Report, Port Usage Report, Raw Meeting Outdial Information (Users) Report, or Raw System Outdial Report to monitor unusual inbound and outbound activity on a trunk. For descriptions and examples of these reports, see Running Reports.