As with your other enterprisewide resources (such as network, e-mail, and voice mail), security is an important issue when installing and configuring Cisco Unified MeetingPlace. Potential threats are posed by outside parties, former employees, and even current employees. As you plan for the security of your system, also consider its overall ease of use.

Areas of security to consider include:

- Unauthorized entrance to legitimate meetings.
- Scheduling and participation in unauthorized meetings.
- Outdialing abuse and toll fraud.
- Unauthorized access to system configuration and parameters through the system manager profile.

In addition to the security parameters in the Cisco Unified MeetingPlace system, your organization can adopt several best practices to greatly enhance security. Your certified installation partner or Cisco Advanced Services representative will describe Cisco Unified MeetingPlace security to you and help you configure the system and develop best practices to ensure a secure conferencing environment.

Use the following guidelines as you establish and maintain security for the system:

- Write and implement a policy regarding user and group profiles, including the security parameter settings from the table in Worksheet 4-1: Security Parameters.
- Keep the number of user profiles with system manager permissions to a minimum. Use longer IDs and passwords for these accounts and change them more frequently.
- If possible, automate the process of adding and deleting user profiles by installing Cisco Unified MeetingPlace Directory Services or manually scripting these actions from your organization's human resources database. Either action ensures that terminated employees' profiles are deleted or deactivated. Your Cisco Unified MeetingPlace support organization can provide further information on both these options.
- If you cannot automate the profile process, write and strictly follow a program of regular, frequent additions and deletions based on information from your organization's human resources group. It is particularly important that user profiles for terminated employees be quickly deactivated or deleted.
- Determine a system of profile numbers that are not easy to guess, but also not difficult for your users to remember. For example, because phone extensions can often be easily guessed, add a prefix. Employee IDs can also be used as long as they are not vulnerable to a random attack. For security purposes, we recommend selecting profile numbers that include at least seven digits.
- Make sure the default profile password cannot be easily guessed, and be sure that users change it quickly. Run regular periodic reports to determine which profile passwords have not been changed from the default and respond by either contacting the user, changing the password, or deactivating or deleting the profile.
- Write and communicate a policy regarding profile passwords so that users do not select trivial passwords. For example, have users refrain from creating passwords that contain repeated or consecutive digits.

- Provide tips to the end-user community regarding how to secure their meetings. Meeting security features include unique meeting IDs, non-trivial meeting IDs, announced entry, meeting passwords, attendance restrictions, locking meetings, deleting unwanted participants, and roll call.
- Write and implement a policy of regular system monitoring for undesired access. Reports and alarms are the primary instruments for such monitoring.
- Plan your responses to different types of unauthorized access. In particular, determine any changes you will make to Cisco Unified MeetingPlace Audio Server security parameters, other system access (such as changing phone numbers), and procedural changes you might make in your organization.
- Keep Cisco Unified MeetingPlace Audio Server behind a firewall in a protected part of the network. There is no need to access the system directly from outside.
- Make sure the TCP port used by MeetingTime (port 5001) is blocked at the firewall. Cisco does not recommend allowing Internet access using MeetingTime.
- Consider installing SSH on the Cisco Unified MeetingPlace 8106 or 8112 and disabling the use of Telnet. Note that SSH is installed separately from the base software release to comply with export regulations. You can find it at http://www.cisco.com/cgi-bin/tablebuild.pl/meetingplace-serv-crypto/. Look for the file called sshpatch.3.1.0.tar.gz

- Consider disabling SNMP queries on Cisco Unified MeetingPlace Audio Server. Note that SNMP traps, indicating alarm conditions, can still be generated even if queries are disabled.
- Make sure the technician ("tech") command line password has been changed from the factory default (username = *admin* ; password = *cisco* ).
- Consider upgrading the various integration application products to use GWSIM 5.0 or higher, particularly those that are placed outside the protected part of the network. GWSIM 5.0 uses an encrypted data stream to communicate with Cisco Unified MeetingPlace Audio Server. It can also communicate with the server using a data stream originating from the server, thus requiring fewer holes in the firewall.