CHAPTER 2

Configuring Security

Before you set up your server for discovering, monitoring, and configuring your Cisco network, you need to make some decisions about the level of security you desire in your network management. With the Cisco Mobile Wireless Transport Manager (MWTM), you can determine how you want users to authenticate, whether you want encrypted data between the application client and the server, and if you want to limit client access to specific IP addresses.

This chapter provides information about configuring MWTM security and limiting access to the MWTM. This chapter contains:

- Configuring User Access, page 2-1
- Implementing SSL Support in the MWTM, page 2-23
- Limiting MWTM Client Access to the MWTM Server (Server Only), page 2-31
- Backing Up or Restoring MWTM Files (Server Only), page 2-32
- Removing MWTM Data from the MWTM Server, page 2-35

Configuring User Access

You can use the MWTM to control who is allowed to do what in the MWTM, beyond simply specifying root and non root users. The MWTM calls this ability user-based access.

User-based access provides multilevel, password-protected access to MWTM features. Each user can have a unique username and password. You can also assign each user to one of five levels of access, which control the list of MWTM features accessible by that user.

To configure MWTM user access, perform the tasks in the following sections. Required and optional tasks are indicated:

Required:

- Implementing Secure User Access (Server Only), page 2-2
- Implementing User Groups, page 2-5
- Creating Secure Passwords, page 2-9
- Configuring MWTM User Account Levels (Server Only), page 2-9

Optional:

- Automatically Disabling Users and Passwords (Server Only), page 2-12
- Manually Disabling Users and Passwords (Server Only), page 2-14
- Enabling and Changing Users and Passwords (Server Only), page 2-15
- Displaying a Message of the Day, page 2-17
- Manually Synchronizing Local MWTM Passwords (Server Only), page 2-18
- Listing All Currently Defined Users (Server Only), page 2-18
- Displaying the Contents of the System Security Log (Server Only), page 2-19
- Restoring Security-Related MWTM Data (Server Only), page 2-20
- Disabling MWTM User-Based Access (Server Only), page 2-20
- Specifying a Super User (Server Only), page 2-21

Implementing Secure User Access (Server Only)

Before you can access the full suite of security commands in the MWTM, you must enable MWTM user access, configure the type of security authentication you want, and add users to your user lists.

After you implement user access for the MWTM, users must log in to the system to access the:

- MWTM client interface
- MWTM web interface
- Event Editor
- Global Title Translation (GTT) Editor (ITP only)
- Address Table Editor (ITP only)

Note After you implement MWTM user access, if a user logs in on one client, then logs in on a second client, the MWTM closes the first client and records the event in the system security log.

Security Authentication

Two types of security authentication are possible:

- *Local authentication*: You can create user accounts and passwords that are local to the MWTM system. When using this method, you can use MWTM user access commands to manage usernames, passwords, and access levels.
- *Solaris/Linux authentication*: Uses standard Solaris- or Linux-based user accounts and passwords, as specified in the */etc/nsswitch.conf* file. You can provide authentication using the local */etc/passwd* file; a distributed Network Information Services (NIS) system; or any other type of authentication tool (for details, see Additional Authentication Tools, page 2-4). You can use all MWTM user access commands except:
  - mwtm disablepass
  - mwtm passwordage
  - mwtm userpass

In addition, if you have enabled Solaris/Linux authentication, you must be logged in as the root user, not as a superuser, to use:

- mwtm adduser
- mwtm updateuser
- mwtm authtype

PAM Setup to Check Library Version and JVM Versions

- To ensure Java Virtual Machine (JVM) version and available Pluggable Authentication Modules (PAM) library matches:
  - If your Operating System only has 32-bit version of the PAM library, then you need to make sure to use 32-bit JVM.
  - If your Operating System only has 64-bit version of the PAM library, then you need to make sure to use 64-bit JVM.
  - If your Operating System has both 32-bit and 64-bit versions of PAM libraries, then you can use either 32-bit or 64-bit JVM.
- To check the available PAM authentication module versions:
  - To check PAM authentication module version on Solaris:

    ```
    file /usr/lib/security/pam_radius_auth.so
    file /usr/lib/security/sparcv9/pam_radius_auth.so
    ```

  - To check PAM authentication module version on Linux:

    ```
    file /lib/security/pam_radius_auth.so
    file /lib64/security/pam_radius_auth.so
    ```

- To check JVM versions, go to:

  /opt/CSCOsgm/j2re/jre/bin/java -version

- To change the JVM version on Solaris:

  On Solaris, MWTM has both 32-bit and 64-bit JVM versions. By default, the MWTM 6.1.7 and above enables 64-bit JVM on Solaris. To change JVM to 32-bit version, enter the following commands:

  ```
  % cd /opt/CSCOsgm/j2re/jre/bin
  % mv java.sgm java.64
  % mv java.32 java.sgm
  % /opt/CSCOsgm/bin/mwtm restart
  ```

  To check if the JVM version is changed successfully, go to:

  /opt/CSCOsgm/j2re/jre/bin/java -version

- To check the JVM version on Linux:

  For Linux, you cannot change JVM versions. MWTM installation program installs 64-bit JVM if the Linux runs 64-bit kernel. MWTM installation program installs 32-bit JVM if the Linux runs 32-bit kernel.

  You need to ensure that proper version of PAM library is available on Linux that matches the kernel version.

Additional Authentication Tools

With the introduction of Pluggable Authentication Modules (PAM) in MWTM 6.1, you can use additional authentication tools, such as Remote Authentication Dial In User Service (RADIUS) or Terminal Access Controller Access-Control System (TACACS+) to log in to MWTM and the network devices that are configured. Thus same User Id and Password can be used to log in to MWTM and the network devices. This can be done by modifying the device credentials and user credentials..

For example, if you want to use RADIUS, follow these steps:

Step 1 Ensure that you have:

- Selected Solaris or Linux authentication, either during installation or using the **mwtm authtype** command (see mwtm authtype, page B-9)
- Download and compile the PAM radius module from the internet (http://freeradius.org/).

Note Check the install subdirectory of the MWTM installation CD image for the notes - INSTALL.pam_radius.txt (for PAM RADIUS module) or INSTALL.pam_tacplus.txt (for TACPLUS module) and precompiled PAM modules.

Step 2 On the MWTM server, copy the PAM radius file (*pam_radius_auth.so*) you downloaded to the /usr/lib/security directory.

Step 3 For Solaris authentication:

a. On the MWTM server, using a text editor, open this file:

```
/etc/pam.conf
```

b. Modify these lines:

```
mwtm-jpam auth required pam_unix_auth.so
mwtm-jpam account required pam_unix_account.so
```

to:

```
mwtm-jpam auth required pam_radius_auth.so
mwtm-jpam account required pam_radius_auth.so
```

For Linux authentication:

a. On the MWTM server, using a text editor, open this file:

```
/etc/pam.d/mwtm-jpam
```

b. Modify these lines (for 32 or 64-bit, respectively):

```
auth required /lib/security/pam_unix_auth.so
account required /lib/security/pam_unix_auth.so
or
auth required /lib64/security/pam_unix_auth.so
account required /lib64/security/pam_unix_auth.so
```

to:

```
auth required /lib/security/pam_radius_auth.so
account required /lib/security/pam_radius_auth.so
or
auth required /lib64/security/pam_radius_auth.so
account required /lib64/security/pam_radius_auth.so
```

Step 4 Enter:

```
cd /etc
```

Step 5 Create the following directory: *raddb.*

Step 6 You should have a PAM configuration file named pam_radius_auth.conf. Copy this file as *server* in the */etc/raddb/* directory.

Step 7 Configure the *server* file you just created with the actual Radius server, port number, and the secret password. For example:

```
172.16.24.60:1812 secret  3
```

Note If a MWTM superuser is defined, user access is enabled with authtype set to solaris or linux, and user accounts for accessing MWTM are maintained locally on the host running the MWTM server, then */etc/shadow* must be readable by the MWTM superuser account:
chown superuser /etc/shadow where *superuser* is the name of the MWTM superuser account.

Note See http://sourceforge.net/projects/tacplus for the details on PAM_TACPLUS module.

Implementing User Groups

User Groups or Datacenters, are the groups that will be assigned a Device Groups that are created based on the personalities. More than one device group can be assigned to each user group or Datacenters. While creating User Groups, if user access is enabled and users are already created, these users can be selected and assigned to this user groups.

To create and manage, the user groups and device groups:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See Becoming the Root User (Server Only), page 3-2
- Super user—See Specifying a Super User (Server Only), page 2-21

Step 2 Enter the following command to create a user group:

```
mwtm usergroups create groupName location [ -d <devicegroup1> <devicegroup2>
<devicegroup...N> ] [ -u <user1> <user2> <user...N ]
```

where **groupName** is the name of the user group and **location** is the location where the user group is created. The following options can be used to assign the device groups and users at the time of creating the user group:

- **-d**, the option to assign the device group to this user group.
- **-u**, the option to assign the users to this user group.

Step 3 To add the device group or users to user group:

```
mwtm usergroups add    groupName [ -d <devicegroup1> <devicegroup2> <devicegroup...N> ] [
-u <user1> <user2> <user...N> ]
```

where **groupName** is the name of the user group and **location** is the location where the user group is created. The following options can be used to assign the device groups and users at the time of creating the user group:

- **-d**, the option to assign the device group to this user group.
- **-u**, the option to assign the users to this user group.

Step 4 To remove the device group or users assigned to user group:

```
mwtm usergroups remove groupName [ -d <devicegroup1> <devicegroup2> <devicegroup...N> ] [
-u <user1> <user2> <user...N> ]
```

where **groupName** is the name of the user group and **location** is the location where the user group is created. The following options can be used to assign the device groups and users at the time of creating the user group:

- **-d**, the option to assign the device group to this user group.
- **-u**, the option to assign the users to this user group.

Step 5 To delete a user group:

```
mwtm usergroups delete groupName1 [ groupName2 ... ]
```

where **groupName1** is the name of the user group.

Step 6 To view the details of a user group:

```
mwtm usergroups detail groupName
```

where **groupName** is the name of the user group.

Step 7 To import a user group:

```
mwtm usergroups import filename
```

where **filename** is the name of the user group.

Step 8 To export a user group:

```
mwtm usergroups export filename
```

where **filename** is the name of the user group.

Step 9 To list all the user groups:

```
mwtm usergroups list
```

Configuring User Levels

You can configure one of seven account levels for each user. Valid levels are:

1. Basic User (Level 1) Access
2. Power User (Level 2) Access
3. Network Operator (Level 3) Access
4. Network Administrator (Level 4) Access
5. System Administrator (Level 5) Access
6. Custom User Level 1 (Level 11) Access

7. Custom User Level 2 (Level 12) Access

For more information about account levels, see Configuring MWTM User Account Levels (Server Only), page 2-9.

Configuring User Passwords

The method that you use for setting user passwords depends on the type of authentication that you configure on the MWTM system (local or solaris).

Local Authentication

If **mwtm authtype** is set to local, the MWTM prompts you to:

- Enter the user password. When setting the password, follow the rules and considerations in Creating Secure Passwords, page 2-9.
- Force the user to change the password at the next login. The default is to not force the user to change the password.

Whenever a user must change a password, the MWTM issues an appropriate message, and prompts for the username and new password.

Solaris/Linux Authentication

If **mwtm authtype** is set to solaris or linux, users cannot change their passwords by using the MWTM client. Instead, they must manage their passwords on the external authentication servers by using Solaris or Linux commands, such as *passwd*.

All new passwords take effect the next time the MWTM automatically synchronizes local MWTM passwords with Solaris or Linux. You can manually synchronize passwords at any time by using the **mwtm syncusers** command. For more information, see mwtm syncusers, page B-90.

Enabling Secure User Access

To enable secure user access for the MWTM:

Step 1 Log in to the MWTM server as the root user (see Starting the MWTM Client, page 3-3).

Step 2 To enable MWTM security, the following prerequisites must be met:

- User access must be enabled.
- The authentication type must be set.
- Users must be added.

The **mwtm useraccess** enable command takes you through all three stages, checking the status of:

1. **mwtm useraccess**—Enabled or disabled.
2. **mwtm authtype**—If you have not already set the mwtm authentication type, you must do so now.
3. **mwtm adduser**—If you have already assigned users, the MWTM asks if you want to use the same user database, or create a new one. If you have not assigned users, you must do so now.

Tip For details on the **mwtm useraccess**, **mwtm authtype**, and **mwtm adduser** commands, see Appendix B, "Command Reference".

Run the mwtm useraccess enable command:

```
cd /opt/CSCOsgm/bin
./mwtm useraccess enable
~text elided~
```

Step 3 To activate your security changes on the MWTM client, restart the MWTM server with the mwtm restart command (see mwtm restart, page B-61). To activate your security changes on the MWTM web interface, clear the browser cache and restart the browser.

Use the remaining procedures in this chapter to further customize your MWTM security system.

Creating Secure Passwords

When setting passwords in the MWTM, the:

- Password must be at least 6 characters, up to 15 characters.
- Password cannot be identical to the username.
- New password cannot be the same as the old password.
- MWTM does not allow users to switch back and forth between two passwords.
- Password cannot be a commonly used word. The MWTM server uses the system dictionary at */usr/share/lib/dict/words* (Solaris) or */usr/share/dict/words* (Linux) to determine whether a word is a commonly used word.

  To use your own dictionary, add a line to the *System.properties* file:

  - To disable the MWTM dictionary and allow common words, add:

    DICT_FILE=/dev/null

  - To use a custom dictionary, add:

    DICT_FILE=*/new-dictionary*

    where *new-dictionary* is the path and filename of the custom dictionary file, such as */users/usr11/words*. Each line in the custom dictionary must contain a single word, with no leading or trailing spaces.

Configuring MWTM User Account Levels (Server Only)

This section describes the user account levels, and the MWTM client and web interface actions that are available at each level:

- Basic User (Level 1) Access, page 2-10
- Power User (Level 2) Access, page 2-10
- Network Operator (Level 3) Access, page 2-11
- Network Administrator (Level 4) Access, page 2-11
- System Administrator (Level 5) Access, page 2-11
- Custom User Level 1 (Level 11) Access, page 2-12
- Custom User Level 2 (Level 12) Access, page 2-12

The account level that includes an action is the *lowest* level with access to that action. The action is also available to all higher account levels. For example, a System Administrator also has access to all Network Administrator actions.

Account levels are based on the action to be performed, not on the target network element. Therefore, if a user can perform an action on one MWTM network element (such as deleting a node), the user can perform the same action on all similar MWTM network elements (such as deleting an interface, signaling point, or linkset).

Note Access to MWTM information and downloads on Cisco.com is already protected by Cisco.com, and is not protected by the MWTM.

To configure the account level for a user, use the **mwtm adduser** command, as described in Implementing Secure User Access (Server Only), page 2-2, or the **mwtm updateuser** or **mwtm newlevel** commands, as described in Enabling and Changing Users and Passwords (Server Only), page 2-15.

Basic User (Level 1) Access

Basic users can view MWTM data, load MWTM files, and use MWTM drill-down menus.

The following MWTM actions in the client and web interfaces are available to basic users:

MWTM Client Interface Actions	MWTM Web Interface Actions
• View the MWTM web interface homepage • Connect to a new server • Apply changes to views • Load the DEFAULT view and existing views, but cannot save them • View and edit preferences • View and manipulate the topology map, save it as a JPEG, but cannot save icon locations • View network elements, events, details, and notes • Load existing event filters, but cannot save them • Print MWTM windows • Launch CiscoWorks	• View the MWTM web interface homepage • View the following administrative pages: – System Information – System Status • View and edit web preferences • View reports

Power User (Level 2) Access

The following MWTM actions in the client and web interfaces are available to power users:

MWTM Client Interface Actions	MWTM Web Interface Actions
• Access all basic (Level 1) user client actions • Acknowledge events • View, change, and save event configurations, but cannot deploy changes • View real-time data and graphs • Edit network elements, events, and views • Unignore network elements and views • Save preferences files, event filters, and views	• Access all basic (Level 1) user web actions • Acknowledge events • View event configurations • View real-time statistics • Delete alarms • Modify alarm severity • Edit groups • Edit notes

Network Operator (Level 3) Access

The following MWTM actions in the client and web interfaces are available to network operators:

MWTM Client Interface Actions	MWTM Web Interface Actions
• Access all basic (Level 1) user and power (Level 2) user client actions • Access troubleshooting features • Ignore/Unignore network elements and views • Poll nodes • Access nodes through Telnet or SSH • (ITP only) View route table files and GTT files, but cannot edit them	• Access all basic (Level 1) user and power (Level 2) user web actions • Access troubleshooting features • Access provisioning features • Access all features on Administrative pages

Network Administrator (Level 4) Access

The following MWTM actions in the client and web interfaces are available to network administrators:

MWTM Client Interface Actions	MWTM Web Interface Actions
• Accessing all basic (Level 1) user, power (Level 2) user, and network operator (Level 3) client actions • Modify and view SNMP configuration • Perform network discovery • Delete network elements • Unmanage nodes • (ITP only) Edit and save route table files, GTT files, and address table files • (ITP only) Use the deployment wizard	• Accessing all basic (Level 1) user, power (Level 2) user, and network operator (Level 3) web actions • Automatically log into SSH terminal in enable mode (if enable password is set)

System Administrator (Level 5) Access

The following MWTM actions in the client and web interfaces are available to system administrators:

MWTM Client Interface Actions	MWTM Web Interface Actions
• Accessing all basic (Level 1) user, power (Level 2) user, network operator (Level 3), and network administrator (Level 4) client actions • Access and modify trap settings • Manage/Unmanage nodes • Deploy saved event configuration changes • PM Mode enable/disable	• Accessing all basic (Level 1) user, power (Level 2) user, network operator (Level 3), and network administrator (Level 4) web actions • Access and modify trap settings • Enable and disable reports (MSU Rates)

Custom User Level 1 (Level 11) Access

The following MWTM actions in the client and web interfaces are available for custom user level 1 users:

MWTM Client Interface Actions	MWTM Web Interface Actions
• Customizing all basic (Level 1) user, power (Level 2) user, network operator (Level 3), network administrator (Level 4), and system administrator (Level 5) client actions.	• Customizing all basic (Level 1) user, power (Level 2) user, network operator (Level 3), network administrator (Level 4), and system administrator web actions.

Custom User Level 2 (Level 12) Access

The following MWTM actions in the client and web interfaces are available for custom user level 2 users:

MWTM Client Interface Actions	MWTM Web Interface Actions
• Customizing all basic (Level 1) user, power (Level 2) user, network operator (Level 3), network administrator (Level 4), and system administrator (Level 5) client actions.	• Customizing all basic (Level 1) user, power (Level 2) user, network operator (Level 3), network administrator (Level 4), and system administrator (Level 5) web actions.

Automatically Disabling Users and Passwords (Server Only)

After you have implemented the basic MWTM security system, you can customize the system to automatically disable users and passwords when certain conditions are met (for example, a series of unsuccessful login attempts or a specified period of inactivity).

Tip To view a list of current users and the status of user accounts, use the **mwtm listusers** command (see mwtm listusers, page B-44).

To automatically disable users and passwords:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See Becoming the Root User (Server Only), page 3-2
- Super user—See Specifying a Super User (Server Only), page 2-21

Step 2 Enter the following command:

```
cd /opt/CSCOsgm/bin
```

Step 3 (Optional) To configure the MWTM to generate an alarm after a specified number of unsuccessful login attempts by a user, enter:

`./mwtm badloginalarm` *number-of-attempts*

where *number-of-attempts* is the number of unsuccessful login attempts allowed before the MWTM generates an alarm.

The valid range is 1 unsuccessful attempt to an unlimited number of unsuccessful attempts. The default value is 5 unsuccessful attempts.

To disable this action (that is, to prevent the MWTM from automatically generating an alarm after unsuccessful login attempts), enter:

```
./mwtm badloginalarm clear
```

Step 4 (Optional) To configure the MWTM to disable a user's account automatically after a specified number of unsuccessful login attempts, enter:

```
# ./mwtm badlogindisable number-of-attempts
```

where *number-of-attempts* is the number of unsuccessful login attempts allowed before the MWTM disables the user's account. The MWTM does not delete the user from the user list, the MWTM only disables the user's account.

The valid range is 1 unsuccessful attempt to an unlimited number of unsuccessful attempts. The default value is 10 unsuccessful attempts.

To re-enable the user's account, use the mwtm enableuser command.

To disable this action (that is, to prevent the MWTM from automatically disabling a user's account after unsuccessful login attempts), enter:

```
# ./mwtm badlogindisable clear
```

Step 5 (Optional) The MWTM keeps track of the date and time each user last logged in. To configure the MWTM to disable a user's log in automatically after a specified number of days of inactivity, enter:

```
# ./mwtm inactiveuserdays number-of-days
```

where *number-of-days* is the number of days that a user can be inactive before the MWTM disables the user's account. The MWTM does not delete the user from the user list, the MWTM only disables the user's account.

The valid range is 1 day to an unlimited number of days. There is no default setting.

To re-enable the user's account, use the mwtm enableuser command.

This action is disabled by default. If you do not specify the mwtm inactiveuserdays command, user accounts are never disabled as a result of inactivity.

If you have enabled this action and you want to disable it (that is, to prevent the MWTM from automatically disabling user accounts as a result of inactivity), enter:

```
# ./mwtm inactiveuserdays clear
```

Step 6 (Optional) If **mwtm authtype** is set to local, you can configure the MWTM to force users to change their passwords after a specified number of days.

To configure the MWTM to force users to change their passwords after a specified number of days, enter:

```
# ./mwtm passwordage number-of-days
```

where *number-of-days* is the number of days allowed before users must change their passwords.

Note You must have changed your password at least once for the **mwtm passwordage** command to properly age the password.

The valid range is 1 day to an unlimited number of days. There is no default setting.

Note The MWTM starts password aging at midnight on the day that you set the value. For example, if you use the **mwtm passwordage** command to set the password age to 1 day (24 hours), the password begins to age at midnight and expires 24 hours later.

This action is disabled by default. If you do not specify the mwtm passwordage command, users never need to change their passwords.

If you have enabled this action and you want to disable it (that is, prevent the MWTM from forcing users to change passwords), enter:

```
# ./mwtm passwordage clear
```

Note If **mwtm authtype** is set to solaris or linux, you cannot use the **mwtm passwordage** command. Instead, you must manage passwords on the external authentication servers.

Step 7 (Optional) To configure the MWTM to automatically disconnect a client (this includes the MWTM client, the GTT editor, and the address table editor) after a specified number of minutes of inactivity, enter:

```
# ./mwtm clitimeout number-of-minutes
```

where *number-of-minutes* is the number of minutes a client can be inactive before the MWTM disconnects the client.

The valid range is 1 minute to an unlimited number of minutes. There is no default value.

This action is disabled by default. If you do not specify the mwtm clitimeout command, clients are never disconnected as a result of inactivity.

If you have enabled this action and you want to disable it (that is, never disconnect a client as a result of inactivity), enter the following command:

```
# ./mwtm clitimeout clear
```

Manually Disabling Users and Passwords (Server Only)

As described in the Automatically Disabling Users and Passwords (Server Only), page 2-12, you can customize the MWTM to automatically disable users and passwords when certain conditions are met. However, you can also manually disable MWTM users and passwords whenever you suspect a security breech has occurred.

To disable MWTM users and passwords:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See Starting the MWTM Client, page 3-3
- Super user—See Specifying a Super User (Server Only), page 2-21

Step 2 Enter:

```
# cd /opt/CSCOsgm/bin
```

Step 3 (Optional) To delete a user entirely from the MWTM user access account list, enter:

```
# ./mwtm deluser username
```

where *username* is the name of the user.

If you later decide to add the user back to the account list, you must use the **mwtm adduser** command.

Step 4 (Optional) If **mwtm authtype** is set to local, you can disable a user's password. To disable a user's password, enter:

```
# ./mwtm disablepass username
```

where *username* is the name of the user. The MWTM does not delete the user from the account list, the MWTM only disables the user's password.

Note If **mwtm authtype** is set to solaris or linux, you cannot use the **mwtm disablepass** command. Instead, you must manage passwords on the external authentication servers.

The user must change the password the next time he or she logs in.

You can also re-enable the user's account with the same password, or with a new password:

- To re-enable the user's account with the same password as before, use the **mwtm enableuser** command.
- To re-enable the user's account with a new password, use the **mwtm userpass** command.

Step 5 (Optional) To disable a user's account, but not the user's password, enter:

```
# ./mwtm disableuser username
```

where *username* is the name of the user.

Note If **mwtm authtype** is set to solaris or linux, you must be logged in as the root user, not as a superuser, to enter this command.

The MWTM does not delete the user from the account list; the MWTM only disables the user's account. The user cannot log in until you re-enable the user's account:

- To re-enable the user's account with the same password as before, use the **mwtm enableuser** command.
- To re-enable the user's account with a new password, use the **mwtm userpass** command.

Enabling and Changing Users and Passwords (Server Only)

Of course, the MWTM also enables you to re-enable users and passwords, and change user accounts. To enable and change users and passwords:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See Starting the MWTM Client, page 3-3
- Super user—See Specifying a Super User (Server Only), page 2-21

Step 2 Enter the following command:

```
# cd /opt/CSCOsgm/bin
```

Step 3 (Optional) To re-enable a user's account, which had been disabled either automatically by the MWTM or by a superuser, enter the following command:

```
# ./mwtm enableuser username
```

where *username* is the name of the user. The MWTM re-enables the user's account with the same password as before.

Note If **mwtm authtype** is set to solaris or linux, you must be logged in as the root user, not as a superuser, to enter this command.

Step 4 (Optional) If **mwtm authtype** is set to local, you can change a user's password, or re-enable the user's account with a new password, if the user's account had been disabled either automatically by the MWTM or by a superuser. To change a password or to re-enable a user's account with a new password, enter:

```
# ./mwtm userpass username
```

where *username* is the name of the user.

The MWTM prompts you for the new password. When setting the password, follow the rules and considerations in the Creating Secure Passwords, page 2-9.

If the user's account has also been disabled, the MWTM re-enables the user's account with the new password.

Note If **mwtm authtype** is set to solaris or linux, you cannot use the **mwtm userpass** command. Instead, you must manage passwords on the external authentication servers.

Step 5 (Optional) To change a user's account level and password, enter the following command:

```
# ./mwtm updateuser username
```

where *username* is the name of the user.

Note If **mwtm authtype** is set to solaris or linux, you must be logged in as the root user, not as a superuser, to enter this command.

The MWTM prompts you for the new account level. Valid levels are described in Configuring User Levels, page 2-6:

If **mwtm authtype** is set to local, the MWTM also prompts you for the user's new password. When setting the password, follow the rules and considerations in Creating Secure Passwords, page 2-9.

Step 6 (Optional) To change a user's account level, but not the user's password, enter the following command:

```
# ./mwtm newlevel username
```

where *username* is the name of the user.

The MWTM prompts you for the new account level. Valid levels are described in Configuring User Levels, page 2-6.

Displaying a Message of the Day

You can use the MWTM to display a user-specified MWTM system notice called the message of the day. You can use the message of the day to inform users of important changes or events in the MWTM system. The message of the day also gives users an opportunity to exit the MWTM client, Event Editor, GTT Editor (ITP only), or Address Table Editor (ITP only) before starting them.

If you enable the message of the day, it appears whenever a user attempts to launch a client. If the user accepts the message, the client launches. If the user declines the message, the client does not launch.

To display the Message of the Day dialog, use one of the following procedures:

- Launch a client. If there is a message of the day, the Message of the Day dialog appears.
- Launch MWTM web client. Choose **Administrative > System Information > Message of the Day**. This link appears only after enabling message of the day using the command mwtm motd.
- Choose **View > Message of the Day** from the MWTM main menu (in case of Java client).
- Select the MWTM server name in the lower-right corner of the MWTM main window.

The Message of the Day dialog contains the following fields:

Field or Button	Description
Message of the Day Last Updated	Date and time the message of the day was last updated. If there is no message of the day, the MWTM displays Unknown.
Message Field	Text of the message of the day. If there is no message of the day, the MWTM displays `There is no message of the day`.
Accept	Closes the Message of the Day dialog and launches the client. If you do not click Accept, you cannot launch the client. This button is available when there is a message of the day and you launch a client.
Decline	Closes the Message of the Day dialog and exits the client. This button is available when there is a message of the day and you launch a client.
OK	Closes the Message of the Day dialog without exiting the client. This button is available if you displayed the Message of the Day dialog by choosing **View > Message of the Day** from the MWTM main menu. The OK button is not available in web client.

To configure the MWTM to display a message of the day:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See Starting the MWTM Client, page 3-3
- Super user—See Specifying a Super User (Server Only), page 2-21

Step 2 Enter the following commands:

```
cd /opt/CSCOsgm/bin
./mwtm motd enable
```

The MWTM displays:

```
Enter location of the message of the day file: [/opt/CSCOsgm/etc/motd]
```

Step 3 To accept the default value, press **Enter**; or type a different location and press **Enter**.

The MWTM displays:

```
Setting Message of the Day File to: [/opt/CSCOsgm/etc/motd]
Message of the Day File set to: [/opt/CSCOsgm/etc/motd]
MWTM server must be restarted for changes to take effect.
```

Step 4 To create the message text (the first time) or edit the existing text, enter:

```
./mwtm motd edit
```

Step 5 To display the contents of the message of the day file, enter:

```
./mwtm motd cat
```

Step 6 To disable the message of the day file, enter:

```
./mwtm motd disable
```

Manually Synchronizing Local MWTM Passwords (Server Only)

If **mwtm authtype** is set to solaris or linux, the MWTM automatically synchronizes local MWTM passwords with the operating system at 1:30 a.m. each night (this setting can be changed using the root crontab). However, you can also manually synchronize passwords at any time.

To manually synchronize local MWTM passwords:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See Starting the MWTM Client, page 3-3
- Super user—See Specifying a Super User (Server Only), page 2-21

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Synchronize the MWTM passwords:

```
./mwtm syncusers
```

The MWTM synchronizes the passwords with Solaris.

Listing All Currently Defined Users (Server Only)

To list all currently defined users in the MWTM User-Based Access account list:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See Starting the MWTM Client, page 3-3
- Super user—See Specifying a Super User (Server Only), page 2-21

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 List all users:

```
./mwtm listusers
```

The MWTM displays the following information for each user:

- Username
- Last time the user logged in
- User's account access level
- User's current account status, such as Account Enabled or Password Disabled

Step 4 To list information for a specific user, enter:

```
./mwtm listusers username
```

where *username* is the name of the user.

Note You can also view user account information on the MWTM User Accounts web page.

Displaying the Contents of the System Security Log (Server Only)

To display the contents of the system security log with PAGER:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See Starting the MWTM Client, page 3-3
- Super user—See Specifying a Super User (Server Only), page 2-21

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Display the security log contents:

```
./mwtm seclog
```

The following security events are recorded in the log:

- All changes to system security, including adding users
- Login attempts, whether successful or unsuccessful, and logoffs
- Attempts to switch to another user's account, whether successful or unsuccessful
- Attempts to access files or resources of higher account level
- Access to all privileged files and processes
- Operating system configuration changes and program changes, at the Solaris level
- MWTM restarts
- Failures of computers, programs, communications, and operations, at the Solaris level

Step 4 To clear the log, enter:

```
./mwtm seclog clear
```

The default path and filename for the system security log file is */opt/CSCOsgm/logs/sgmSecurityLog.txt*. If you installed the MWTM in a directory other than */opt*, then the system security log file is located in that directory.

Note You can also view the system security log on the MWTM System Security Log web page. For more information, see Viewing the Security Log, page 12-11.

Restoring Security-Related MWTM Data (Server Only)

If you inadvertently delete your user accounts, or make other unwanted changes to your MWTM security information, the MWTM can restore the security-related parts of the MWTM data files from the previous night's backup.

To restore the security-related MWTM data files:

Step 1 Log in as the root user (for details see Starting the MWTM Client, page 3-3).

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Restore the security-related data:

```
./mwtm restore security
```

The MWTM restores the data.

Disabling MWTM User-Based Access (Server Only)

To completely disable MWTM User-Based Access:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See Starting the MWTM Client, page 3-3
- Super user—See Specifying a Super User (Server Only), page 2-21

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Disable user-based access:

```
./mwtm useraccess disable
```

The MWTM user access is disabled the next time you restart the MWTM server (using the mwtm restart command).

Specifying a Super User (Server Only)

You can use the MWTM to specify a *superuser*. A superuser can perform most actions that otherwise require the user to be logged in as the root user. (The root user can still perform those actions, too.) If you specify a superuser, the server also runs as the superuser and not as the root user.

Caution As a superuser, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are a relatively inexperienced UNIX user, limit your activities as a superuser to the tasks described in this document.

When you specify a superuser, remember that:

- The user must exist in the local */etc/passwd* file. You cannot specify a user that is defined in a distributed Network Information Services (NIS) system.
- The superuser does not have access to all MWTM commands; you must still be logged in as the root user to enter certain commands. You must still be logged in as the root user to enter the following commands:
  - mwtm authtype
  - mwtm backup
  - mwtm backupdir
  - mwtm browserpath
  - mwtm certgui
  - mwtm certtool
  - mwtm clean
  - mwtm cleanall
  - mwtm cleandb
  - mwtm cwsetup
  - mwtm evilstop
  - mwtm jspport
  - mwtm keytool
  - mwtm killclients
  - mwtm reboot
  - mwtm restore
  - mwtm restoreprops
  - mwtm setpath, if you are specifying a *username*
  - mwtm sounddir
  - mwtm ssl

  - mwtm stopclients
  - mwtm superuser
  - mwtm syncusers
  - mwtm termproxy
  - mwtm trapsetup
  - mwtm uninstall
  - mwtm webport
  - mwtm xtermpath
- If the **mwtm authtype** is set to solaris or linux, you must still be logged in as the root user to enter the following commands:
  - mwtm adduser
  - mwtm disablepass
  - mwtm passwordage
  - mwtm updateuser
  - mwtm userpass
- If the SNMP trap port number on the MWTM server is less than 1024, you cannot use the **mwtm superuser** command. To correct this situation, you must specify a new SNMP trap port number that is greater than 1024:
  - To change the SNMP trap port number in the nodes in your network, use the snmp-server host command. By default, the MWTM listens for traps from trap multiplexing nodes and NMS applications on port 44750, so that is a good port number to choose. The SNMP trap port number must be the same on all nodes in your network.
  - For more information, see the description of the snmp-server host command in the "Node Requirements" section of the *Installation Guide for Cisco Mobile Wireless Transport Manager 6.1.7*.
  - Use the **mwtm trapsetup** command to change the SNMP trap port number in the MWTM server to match the port number in the nodes in your network. For more information, see mwtm trapsetup, page B-93.

To specify a superuser on the MWTM server:

Step 1 Log in as the root user (see Becoming the Root User (Server Only), page 3-2).

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Specify the superuser:

```
./mwtm superuser username
```

where *username* is the name of the user.

Implementing SSL Support in the MWTM

Note If you chose the Solaris or Linux authentication options (during installation or through the **mwtm authtype** command) you must enable SSL. For details on the **mwtm authtype** command, see mwtm authtype, page B-9.

You can implement Secure Sockets Layer (SSL) support in your MWTM system. When you do, the MWTM uses secure sockets to encrypt all communication between the MWTM clients and server.

This section includes the following information:

- Enabling SSL Support on the MWTM Server, page 2-23
- Downloading the MWTM SSL Module for Windows Using the Web Interface, page 2-25
- Downloading the Self-Signed SSL Certificate from the MWTM Server, page 2-25
- Launching the MWTM Certificate Tool for SSL, page 2-26
- Exporting an SSL Certificate, page 2-28
- Viewing Detailed Information About a SSL Certificate, page 2-28
- Managing SSL Support in the MWTM, page 2-29
- Disabling SSL Support in the MWTM, page 2-30

Enabling SSL Support on the MWTM Server

To enable SSL support in the MWTM, perform the following:

Step 1 Install an SSL key/certificate pair in the MWTM by using one of the following procedures:

- To install a new SSL key and a self-signed certificate, generate the key and certificate by logging in as the root user on the MWTM server and entering the **mwtm keytool genkey** command.

  The MWTM stops the MWTM server and these prompts appear:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
Certificate Validity (number of days)? [min: 30, default: 365]
```

  Enter the requested information.

  The MWTM generates the following files:

  - */opt/CSCOsgm/etc/ssl/server.key* is the MWTM server's private key. Ensure that unauthorized personnel cannot access this key.
  - */opt/CSCOsgm/etc/ssl/server.crt* is the self-signed SSL certificate.
  - */opt/CSCOsgm/etc/ssl/server.csr* is a certificate signing request (CSR). It is not used if you are using a self-signed SSL certificate.

- To install a new SSL key and a certificate signed by a certificate authority (CA), generate the key and a CSR by logging in as the root user on the MWTM server and entering the **mwtm keytool genkey** command.

  The MWTM stops the MWTM server and issues the following prompts:

  ```
  Country Name (2 letter code) []:
  State or Province Name (full name) []:
  Locality Name (eg, city) []:
  Organization Name (eg, company) []:
  Organizational Unit Name (eg, section) []:
  Common Name (your hostname) []:
  Email Address []:
  Certificate Validity (number of days)? [min: 30, default: 365]
  ```

  Enter the requested information.

  The MWTM generates the following files:

  - */opt/CSCOsgm/etc/ssl/server.key* is the MWTM server's private key. Ensure that unauthorized personnel cannot access this key.
  - */opt/CSCOsgm/etc/ssl/server.csr* is a CSR.
  - */opt/CSCOsgm/etc/ssl/server.crt* is the self-signed SSL certificate. It is not used if you are using a CA-signed SSL certificate; the CA-signed certificate overrides the self-signed certificate.

  Print the CSR in X.509 format, by logging in as the root user on the MWTM server and entering the **mwtm keytool print_csr** command.

  Send the CSR to a CA to be signed.

  After the CA signs the certificate, log in as the root user on the MWTM server and enter the following command:

  ./mwtm keytool import_cert *cert_filename*

  where *cert_filename* is the name of the signed certificate.

  The MWTM stops the MWTM server and imports the certificate in X.509 format.

- To use an existing signed key/certificate pair, log in as the root user on the MWTM server and enter the following command:

  ./mwtm keytool import_key *key_filename cert_filename*

  where *key_filename* is the name of the existing SSL key and *cert_filename* is the name of the existing signed certificate.

  The MWTM stops the MWTM server and imports the SSL key in OpenSSL format and the signed SSL certificate in X.509 format.

Step 2 Enable SSL support in the MWTM, by logging in as the root user on the MWTM server and entering the **mwtm ssl enable** command.

Step 3 Restart the MWTM server.

Step 4 Set up the MWTM client-side SSL certificate trust relationship by downloading and importing the self-signed or CA-signed certificate on every remote MWTM client, Windows as well as Solaris, that connects to the MWTM server.

a. (Self-signed certificate only) Download the self-signed certificate (*server.crt*) by using the procedure in Downloading the Self-Signed SSL Certificate from the MWTM Server, page 2-25.

b. Import the self-signed or CA-signed certificate by using the procedure in Launching the MWTM Certificate Tool for SSL, page 2-26.

Step 5 Restart the MWTM client.

The MWTM clients can now connect to the MWTM server by using SSL. All communication between the server and clients is encrypted.

If an MWTM client, GTT editor (ITP only), or Address Table editor (ITP only) that is not SSL-enabled attempts to connect to an SSL-enabled MWTM server, the MWTM displays an appropriate warning message and opens the MWTM Client for Windows page. You can then download and install a new MWTM SSL module for the client to use to connect to that MWTM server.

If the client is SSL-enabled but does not have the correct certificate, the MWTM displays an appropriate warning message and opens the MWTM Server SSL Certificate page. You can then download the signed SSL certificate in X.509 format to the client.

Downloading the MWTM SSL Module for Windows Using the Web Interface

To install the MWTM SSL module on a Windows system from the MWTM web interface:

Step 1 From your browser, go to the URL for the MWTM Homepage:

`http://your_mwtm_server:1774`

where *your_mwtm_server* is the name or IP address of the MWTM server and *1774* is the web port being used by the MWTM (**1774** is the default port number.) If you do not know the name or web port of the MWTM server, contact the system administrator who installed the MWTM server software.

The MWTM web interface home page appears.

Step 2 Click **Download Windows Client**. Ensure that your browser is pointed to an MWTM, SSL-enabled server.

Step 3 Right-click **Download SSL Module for MWTM Client on Windows XP** and choose the **Save Link As** or **Save Target As** option.

Note If you are using Internet Explorer, change the *.zip* extension to *.jar* during the Save Target As option.

Step 4 When queried, save the file under *<Installed Drive>:\Program Files\Cisco Systems\MWTMClient\lib* where *<Installed Drive>* is the disk on which the MWTM client is installed.

Step 5 You are prompted to launch the client, then download the self-signed SSL certificate (follow the subsequent procedures).

Downloading the Self-Signed SSL Certificate from the MWTM Server

If you have implemented Secure Sockets Layer (SSL) support in your MWTM system, you can download the MWTM server's signed SSL certificate to all remote MWTM clients that connect to the server using SSL.

To download the certificate from the MWTM Server SSL Certificate page, use the following procedure on each remote MWTM client:

Step 1 In a web browser, enter the following URL:

```
https://server_name:1774
```

where *server_name* is the name or IP address of the server on which the MWTM server is running and *1774* is the Web port being using by the MWTM (**1774** is the default port number.) If you do not know the name or Web port of the MWTM server, contact the system administrator who installed the MWTM server software.

The Server SSL Certificate page appears.

Step 2 Right-click **Download Server SSL Certificate**.

Step 3 Select **Save Link As** (or **Save Target As**) from the right-click menu.

Step 4 Select a directory in which to save the certificate (*server.crt*), and click **Save**.

The MWTM downloads the *server.crt* file into the specified directory.

Launching the MWTM Certificate Tool for SSL

If you have implemented Secure Sockets Layer (SSL) support in your MWTM system, you can launch the MWTM Certificate Tool for SSL. The MWTM Certificate Tool dialog box lists all SSL certificates that the MWTM client imported. In this dialog box, you specify whether to import, export, and display detailed information about SSL certificates.

To launch the MWTM SSL Certificate Tool, use one of the following procedures:

- In Solaris, log in as the root user and enter the following commands:

```
cd /opt/CSCOsgm/bin
./mwtm certgui
```

  For more information, see mwtm certgui, page B-14.

- In Windows, choose **Start > Programs > Cisco MWTM Client > MWTM SSL Certificate Tool**.

The MWTM displays the MWTM Certificate Tool dialog box.

For each SSL certificate, the MWTM Certificate Tool dialog box displays:

Field or Button	Description
Issued to	Hostname of the MWTM server to which the SSL certificate was issued.
Issued by	Certificate authority (CA) that issued the SSL certificate. Self-signed SSL certificates display the hostname of the MWTM server.
Expiration Date	Date on which the SSL certificate expires.
Import	Displays the Open dialog box for an SSL certificate, which you use to import SSL certificates (for details, see Importing an SSL Certificate to an MWTM Client, page 2-27).
Export	Displays the Save dialog box for an SSL certificate, which you use to export the selected SSL certificate.
Remove	Removes the selected SSL certificate from the table.
Details	Displays the Certificate Information dialog box, which provides detailed information about the selected certificate.

Field or Button	Description
Exit	Closes the MWTM Certificate Tool dialog box.
Help	Displays online help for the current window.

Importing an SSL Certificate to an MWTM Client

If you have implemented Secure Sockets Layer (SSL) support in your MWTM system, you can import the MWTM server's self-signed SSL certificate, or a CA-signed SSL certificate, to all remote MWTM clients that connect to the server using SSL.

Note If you are using a Solaris client, you can import by using the MWTM SSL Certificate Tool as described in this section, or the CLI command **mwtm certtool** (for details, see mwtm certtool, page B-15). If you are using a Windows client, you must use the MWTM SSL Certificate Tool.

To import an SSL certificate, launch the MWTM SSL Certificate Tool, as described in Launching the MWTM Certificate Tool for SSL, page 2-26, then click **Import**. The MWTM displays the Open dialog box for SSL certificates.

Use the Open dialog box to locate the SSL certificate that you want to import. The Open dialog box contains:

Field or Button	Description
Look In	Click to select the directory in which you want to find the SSL certificate. Accept the default directory, or select a new directory from the drop-down list box. For a self-signed certificate, locate the directory in which you downloaded the certificate.
File Name	Enter a name for the SSL certificate, or select a file from those listed in the "Open" field. The MWTM displays the name of the certificate in the "File Name" field.
Files of Type	Specifies the type of file to display, and displays all files of that type in the selected directory. For SSL certificates, this field displays "All files," which means files of all types appear in the table.
 Up One Level	Displays the subfolders and files that are in the folder that is up one level from the currently visible folder.
 Desktop	Displays the subfolders and files that are on your workstation desktop.
 Create New Folder	Creates a new subfolder in the visible folder.
 List	Displays only icons for subfolders and files.
 Details	Displays detailed information for subfolders and files, including their size, type, date they were last modified, and so on.
Open	Imports the file, closes the Open dialog box for an SSL certificate, and populates the MWTM Certificate Tool dialog box with the SSL certificate's information.
Cancel	Closes the Open dialog box for an SSL certificate without importing the file.

Exporting an SSL Certificate

If you have implemented Secure Sockets Layer (SSL) support in your MWTM system, you can export SSL certificates that have been imported to the MWTM client.

To export a SSL certificate, launch the MWTM SSL Certificate Tool, as described in Launching the MWTM Certificate Tool for SSL, page 2-26, select a certificate from the list, then click **Export**. The MWTM displays the Save dialog for SSL certificates.

Use the Save dialog box to export the SSL certificate to another directory. The Save dialog box contains:

Field or Button	Description
Save In	Click to select the directory in which you want to save the SSL certificate. Accept the default directory, or select a new directory from the drop-down list box. For a self-signed certificate, locate the directory in which you downloaded the certificate.
File Name	Enter a name for the SSL certificate, or select a file from those listed in the "Save In" field. The MWTM displays the name of the certificate in the "File Name" field.
Files of Type	Specifies the type of file to save, and displays all files of that type in the selected directory. For SSL certificates, this field displays "All files," which means files of all types.
 Up One Level	Displays the subfolders and files that are in the folder that is up one level from the currently visible folder.
 Desktop	Displays the subfolders and files that are on your workstation desktop.
 Create New Folder	Creates a new subfolder in the visible folder.
 List	Displays only icons for subfolders and files.
 Details	Displays detailed information for subfolders and files, including their size, type, date they were last modified, and so on.
Save	Saves the file, closes the Save dialog box for an SSL certificate, and returns to the MWTM Certificate Tool dialog box. Click **Exit** to close the MWTM Certificate Tool dialog box and export the self-signed SSL certificate in X.509 format.
Cancel	Closes the Save dialog for an SSL certificate without saving the file.

Related Topics

Launching the MWTM Certificate Tool for SSL, page 2-26

Viewing Detailed Information About a SSL Certificate

If you implemented Secure Sockets Layer (SSL) support in your MWTM system, you can view detailed information about SSL certificates that were imported to the MWTM client.

To view detailed information about an SSL certificate, use one of the following procedures:

- Click the locked padlock icon in the lower-left corner of any MWTM window.
- Launch the MWTM SSL Certificate Tool, as described in Launching the MWTM Certificate Tool for SSL, page 2-26, select an SSL certificate from the list and click **Details**.

The MWTM displays the Certificate Information dialog.

For the selected SSL, the Certificate Information dialog box displays:

Field or Button	Description
Subject	Node to which the SSL certificate was issued. This field always includes the Common Name (CN) of the subject, which must match the fully qualified hostname of your MWTM server, such as *xxxx.company.com*. This field might also contain other information, such as the Country (C), Organizational Unit (OU), or Organization (O) of the subject.
Issuer	CA that issued the SSL certificate. This field might include the Common Name (CN) of the issuer, as well as the Country (C), Organizational Unit (OU), or Organization (O) of the issuer.
Version	Version of the SSL certificate, such as "V1."
Serial number	Serial number associated with the SSL certificate.
Signature algorithm	Asymmetric algorithm ensures that the digital signature is secure, such as "MD5withRSA."
Valid from	Date and time on which the SSL certificate was created or became valid.
Valid to	Date and time on which the SSL certificate expires.
Public key	Public key associated with the SSL certificate, used for encryption and for verifying signatures.
OK	Closes the Certificate Information dialog box. When you are ready to close the dialog box, click **OK**. The MWTM closes the Certificate Information dialog. If necessary, click **Exit** to close the MWTM Certificate Tool dialog.

Related Topic

Launching the MWTM Certificate Tool for SSL, page 2-26

Managing SSL Support in the MWTM

You use the MWTM to manage SSL support. To:

- Display the current status of SSL support in the MWTM, including whether SSL support is enabled or disabled and which SSL keys and certificates exist, use either the **mwtm ssl status** or **mwtm sslstatus** command.
- Print the MWTM server's SSL certificate in X.509 format, use the **mwtm keytool print_crt** command.
- List the SSL key/certificate pair on the MWTM server, use the **mwtm keytool list** command.
- List all SSL certificates on the MWTM client, launch the MWTM SSL Certificate Tool. The MWTM lists each imported certificate, including to whom the certificate was issued, who issued the certificate, and when the certificate expires.

For more information on the use of these commands, see Appendix B, "Command Reference".

For more information on launching the MWTM SSL Certificate Tool, see Exporting an SSL Certificate, page 2-28.

See Enabling SSL for the Firefox Web Client, page 2-30 for information on using Firefox 3.

Enabling SSL for the Firefox Web Client

If you are using Firefox 3 to connect to an MWTM server that has SSL enabled, you must add an exception to allow the connection to the server.

The first time you attempt to connect to an SSL-enabled MWTM server using Firefox 3, you get an error saying that you're speaking plain HTTP to an SSL-enabled server port. Follow these steps to add an exception to allow the connection:

Step 1 On the Server Connection Failed page, click the link at the bottom to add an exception.

Step 2 In the Add Security Exception form, in the Location field, enter the MWTM server in the form of **https://***<server_name>:1774*/ where *server_name* is the name or IP address of the server on which the MWTM server is running and *1774* is the Web port being using by the MWTM (1774 is the default port number.)

Step 3 Click **Get Certificate**.

Step 4 Click **Confirm Security Exception**.

You can now use Firefox 3 to connect to an SSL-enabled MWTM server.

Disabling SSL Support in the MWTM

You use the MWTM to disable SSL support in the MWTM, and to remove SSL keys and certificates from the MWTM server and clients. To:

- Disable SSL support in the MWTM, use the **mwtm ssl disable** command.

  For more information, see mwtm ssl, page B-79.

- Remove all SSL keys and certificates from the MWTM server, use the **mwtm keytool clear** command. The MWTM stops the MWTM server, if necessary, and removes the keys and certificates. Before restarting the server, you must generate new SSL keys by using the **mwtm keytool genkey** command, or you must completely disable SSL using the **mwtm ssl disable** command.

  For more information on the use of these commands, see Appendix B, "Command Reference".

- Remove an SSL certificate from the MWTM client, launch the MWTM SSL Certificate Tool. The MWTM lists each imported certificate. Select the certificate that you want to remove, and click **Remove**. The MWTM deletes the certificate from the list.

  For more information on launching the MWTM SSL Certificate Tool, see Exporting an SSL Certificate, page 2-28.

Limiting MWTM Client Access to the MWTM Server (Server Only)

By default, when you first install the MWTM, all MWTM client IP addresses can connect to the MWTM server. However, you use the MWTM to limit client access to the server by creating and maintaining the *ipaccess.conf* file.

You can create the *ipaccess.conf* file and populate it with a list of MWTM client IP addresses that can connect to the MWTM server. The MWTM allows connections from only those clients, plus the local host. If the file exists but is empty, the MWTM allows connections only from the local host. (The MWTM always allows connections from the local host.)

When you first install the MWTM, the *ipaccess.conf* file does not exist and the MWTM allows all client IP addresses to connect to the MWTM server.

To create the *ipaccess.conf* file and work with the list of allowed client IP addresses:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See Becoming the Root User (Server Only), page 3-2
- Super user—See Specifying a Super User (Server Only), page 2-21

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Create the *ipaccess.conf* file:

- To create the *ipaccess.conf* file and add a client IP address to the list, enter:

  ```
  ./mwtm ipaccess add
  ```

- To create the *ipaccess.conf* file and open the file to edit it directly, enter:

  ```
  ./mwtm ipaccess edit
  ```

The default directory for the file is located in the MWTM installation directory:

- If you installed the MWTM in the default directory, */opt*, then the default directory is */opt/CSCOsgm/etc*.
- If you installed the MWTM in a different directory, then the default directory is located in that directory.

In the *ipaccess.conf* file, begin all comment lines with a pound sign (#).

All other lines in the file are MWTM client IP addresses, with one address per line.

Wildcards (*) are allowed, as are ranges (for example, 1-100). For example, if you input the address ***.*.*.*** then all clients can connect to the MWTM server.

Step 4 After you create the *ipaccess.conf* file, you can use the full set of mwtm ipaccess keywords to work with the file:

- clear—Remove all client IP addresses from the *ipaccess.conf* file, and allow connections from any MWTM client IP address.
- list—List all client IP addresses currently in the *ipaccess.conf* file. If no client IP addresses are listed (that is, the list is empty), connections from any MWTM client IP address are allowed.
- rem—Remove the specified client IP address from the *ipaccess.conf* file.
- sample—Print out a sample *ipaccess.conf* file.

For more information, see mwtm ipaccess, page B-42.

Any changes you make to the *ipaccess.conf* file take effect when you restart the MWTM server.

You can also use the MWTM to limit the IP addresses that can send traps to the server by creating and maintaining the *trapaccess.conf* file. For more information, see the Limiting Traps by IP Address.

Backing Up or Restoring MWTM Files (Server Only)

The MWTM automatically backs up all MWTM data files to the MWTM installation directory daily at 2:30 a.m.

To change the time at which the MWTM automatically backs up files, log in as the root user and change the *root crontab* file:

- **crontab -l** lists cron jobs.
- **crontab -e** opens up an editor so you can make changes and save them.

Note The MWTM performs a database integrity check during the backup. If the check fails, the previous backup is not be overwritten, and the MWTM creates a new failed file (for example: *mwtm61-server-backup-failed.tar.Z*).

This section contains these topics:

- Backing Up MWTM Data Files, page 2-32
- Changing the Backup Directory, page 2-33
- Setting the Number of Backup Days, page 2-33
- Restoring MWTM Data Files, page 2-34

Backing Up MWTM Data Files

To manually back up the MWTM data files at any time on a Solaris or Linux server:

Step 1 Log in as the root user. See Becoming the Root User (Server Only), page 3-2.

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Back up the MWTM files:

```
./mwtm backup
```

The MWTM backs up the data files in the installation directory.

If you installed the MWTM in the default directory, */opt*, then the default backup directory is also */opt*. If you installed the MWTM in a different directory, then the default backup directory is that directory.

Changing the Backup Directory

To change the directory in which the MWTM stores its nightly backup files:

Step 1 Log in as the root user. See Becoming the Root User (Server Only), page 3-2.

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Change the backup directory location:

`./mwtm backupdir` *directory*

where *directory* is the new backup directory.

If the new directory does not exist, the MWTM does not change the directory, but issues an appropriate warning message.

Setting the Number of Backup Days

To set the number of days that the MWTM saves backup files:

Step 1 Log in as the root user. See Becoming the Root User (Server Only), page 3-2.

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Change the number of backup days (default is 1):

```
./mwtm backupdays

Current value is: 1

Enter number of days to save backup files (1-30): [1]
```

Step 4 Enter a value for the number of days from 1 to 30. For example:

```
Enter number of days to save backup files (1-30): [1] 5

Setting number of days to save backup files to 5 days.
```

The MWTM will save backup files for the number of days that you entered. In this example, the MWTM saves backup files for the last five days, and deletes backup files that are older than five days.

Note If the number of backup days is greater than one, then MWTM will automatically zip the older backup files.

Restoring MWTM Data Files

You can restore data files on the same Solaris or Linux server, or on a different Solaris or Linux server running the MWTM 6.1.7.

To restore the MWTM data files from a previous backup:

Step 1 Log in as the root user. See Becoming the Root User (Server Only), page 3-2.

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Restore the MWTM data files:

```
./mwtm restore
```

The MWTM restores the data files.

Note If the number of backup days has been set to more than one day (see Setting the Number of Backup Days, page 2-33), the MWTM will prompt you for a server or client backup file to restore from (because there would be more than one backup file to choose from).

Warning **Do not interrupt this command. Doing so can corrupt your MWTM data files.**

The **mwtm restore** command provides optional keywords that you use to restore only selected MWTM data files, such as GTT files (ITP only), route table files (ITP only), log files, report files, or security files. For more information, see mwtm restore, page B-61.

Removing MWTM Data from the MWTM Server

If you ever want to remove all MWTM data from the MWTM server without uninstalling the product, you can do so in one of two ways. Both ways restore the MWTM server to a state that would exist after a new installation of the MWTM.

Method 1

To remove all MWTM data from the MWTM server, *excluding* message log files, backup files, and report files:

Step 1 Log in as the root user (see Becoming the Root User (Server Only), page 3-2).

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Remove the MWTM data:

```
./mwtm clean
```

Data removed includes all MWTM data, notes, preferences, security settings, route files (ITP only), GTT files (ITP only), address table files (ITP only), seed files, event filters, report control files, and views, as well as any user-created files stored in the MWTM directories.

Method 2

To remove all MWTM data from the MWTM server, including all view files, notes that are associated with network elements, and event filters and preferences, excluding message log files, backup files, report files, configuration settings, and security settings:

Step 1 Log in as the root user. See Becoming the Root User (Server Only), page 3-2.

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgm/bin
```

Step 3 Enter:

```
# ./mwtm cleandb
```

This command restores the MWTM server to a state that would exist after a new installation of the MWTM, except for the presence of the retained files. Data removed includes all MWTM data, notes, preferences, route files (ITP only), GTT files (ITP only), address table files (ITP only) and views, as well as any user-created files stored in the MWTM directories.

To remove all MWTM data from the MWTM server, **including** message log files, backup files, and report files, log in as the root user, as described in the Becoming the Root User (Server Only), page 3-2, then enter the following commands:

```
# cd /opt/CSCOsgm/bin
# ./mwtm cleanall
```

Data removed includes all MWTM data, notes, preferences, security settings, route files (ITP only), GTT files (ITP only), address table files (ITP only), seed files, event filters, report control files, views, message log files, backup files, and report files, as well as any user-created files stored in the MWTM directories.