CHAPTER 10

Configuring MWTM Security

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

- Configuring MWTM User-Based Access, page 10-1
- Implementing SSL Support in MWTM (Solaris Only), page 10-22
- Limiting MWTM Client Access to the MWTM Server (Server Only), page 10-32

Configuring MWTM User-Based Access

MWTM enables you to control who is allowed to do what in MWTM, beyond simply specifying root and non-root users. MWTM calls this ability User-Based Access.

User-Based Access provides multi-level password-protected access to MWTM features. Each user can have a unique user name and password. Each user can also be assigned to one of five levels of access, which control the list of MWTM features accessible by that user.

To configure MWTM User-Based Access, perform the tasks in the following sections. Required and optional tasks are indicated.

- Implementing MWTM User-Based Access (Server Only), page 10-2 (Required)
- Creating Secure Passwords, page 10-5 (Required)
- Configuring MWTM User Authentication Levels (Server Only), page 10-6 (Required)
- Automatically Disabling Users and Passwords (Server Only), page 10-8 (Optional)
- Manually Disabling Users and Passwords (Server Only), page 10-11 (Optional)
- Enabling and Changing Users and Passwords (Server Only), page 10-13 (Optional)
- Displaying a Message of the Day (Server Only), page 10-15 (Optional)
- Manually Synchronizing Local MWTM Passwords (Server Only), page 10-17 (Optional)
- Listing All Currently Defined Users (Server Only), page 10-17 (Optional)
- Displaying the Contents of the System Security Log (Server Only), page 10-18 (Optional)
- Restoring Security-Related MWTM Data (Server Only), page 10-19 (Optional)
- Disabling MWTM User-Based Access (Server Only), page 10-19 (Optional)
- Specifying a Super User (Server Only), page 10-19 (Optional)

Implementing MWTM User-Based Access (Server Only)

Before you can access MWTM's full suite of security commands, you must enable MWTM User-Based Access, configure the type of security authentication you want to use, and begin adding users to your authentication lists.

To implement MWTM User-Based Access, use the following procedure:

Step 1 Log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, or as a super user, as described in the "Specifying a Super User (Server Only)" section on page 10-19.

Step 2 Enter the following commands:

```
# cd /opt/CSCOsgm/bin

# ./mwtm useraccess enable
```

MWTM User-Based Access is enabled the next time you restart the MWTM server.

Step 3 If you have already configured the type of MWTM security authentication you want to use, skip to Step 4.

Otherwise, configure the type of MWTM security authentication you want to use:

- *Local authentication* allows you to create user accounts and passwords local to the MWTM system. When using this method, you can use MWTM User-Based Access commands manage user names, passwords, and access levels.

  To enable local authentication, enter the following command:

  ```
  # ./mwtm authtype local
  ```

- *Solaris/Linux authentication* uses standard Solaris/Linux-based user accounts and passwords, as specified in the */etc/nsswitch.conf* file. Authentication can be provided by the local */etc/passwd* file or from a distributed Network Information Services (NIS) system. You can use all MWTM User-Based Access commands except the following commands:
  - **mwtm disablepass**
  - **mwtm passwordage**
  - **mwtm userpass**

  You must use Solaris/Linux commands, such as **passwd**, to manage passwords.

  Users also cannot change their passwords using the MWTM client. Instead, they must manage their passwords on the external authentication servers, using Solaris/Linux commands, such as **passwd**.

  All new passwords take effect the next time MWTM automatically synchronizes local MWTM passwords with Solaris/Linux, or you can manually synchronize passwords at any time using the **mwtm syncusers** command.

  In addition, if you have enabled Solaris/Linux authentication, you must be logged in as the root user, not as a super user, to use the following MWTM commands:
  - **mwtm adduser**
  - **mwtm disableuser**
  - **mwtm enableuser**
  - **mwtm updateuser**

To enable Solaris/Linux authentication, enter one of the following commands:

```
# ./mwtm authtype solaris
```

or

```
# ./mwtm authtype linux
```

depending upon which platform your MWTM server is running.

See the "MWTM Command Reference" section on page C-1 for more information on the use of each of the above MWTM commands.

Step 4 To add a user to your MWTM User-Based Access authentication list, use the following command:

```
# ./mwtm adduser 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 super user, to enter this command.

MWTM also prompts you for the authentication level for the user. Valid levels are:

- **1**—Basic User
- **2**—Power User
- **3**—Network Operator
- **4**—Network Administrator
- **5**—System Administrator

For more information about authentication levels, see the "Configuring MWTM User Authentication Levels (Server Only)" section on page 10-6.

If **mwtm authtype** is set to **local**, MWTM also issues the following prompts:

- MWTM prompts you for the user's password. When setting the password, follow the rules and considerations in the "Creating Secure Passwords" section on page 10-5.
- MWTM asks whether you want to force the user to change the password at the next login. The default is not to force the user to change the password.

(Whenever a user needs to change a password, MWTM issues an appropriate message and prompts for the user name and new password.)

Note If **mwtm authtype** is set to **solaris** or **linux**, users cannot change their passwords using the MWTM client. Instead, they must manage their passwords on the external authentication servers, using Solaris/Linux commands, such as **passwd**. All new passwords take effect the next time MWTM automatically synchronizes local MWTM passwords with Solaris/Linux, or you can manually synchronize passwords at any time using the **mwtm syncusers** command. See the "mwtm syncusers" section on page C-67 for more information.

At this point, you have implemented your basic MWTM User-Based Access. Users must now log in before using the MWTM client and MWTM Web-based functions. Use the remaining procedures in this section to customize your MWTM security system.

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

Creating Secure Passwords

When setting passwords in MWTM, keep in mind the following rules and considerations:

- The password must be at least 6 characters, up to an unlimited number of characters. However, passwords longer than 15 characters are not recommended.
- The password cannot be identical to the user name.
- The new password cannot be the same as the old password.
- MWTM does not allow users to switch back-and-forth between two passwords.
- The password cannot be a common word. MWTM uses the dictionary located at */usr/lib/share/dict/words* to determine whether a word is common. To override the MWTM dictionary, change the DICT_FILE entry in the *System.properties* file:
  - To disable the MWTM dictionary and allow common words, change the DICT_FILE entry to:

    DICT_FILE=/dev/null
  - To use a custom dictionary, change the DICT_FILE entry to:

    DICT_FILE=/*new-dictionary*

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

Configuring MWTM User Authentication Levels (Server Only)

This section describes the user authentication levels in MWTM, and the MWTM functions and Web displays available at each level:

- Basic User (Level 1) Access, page 10-6
- Power User (Level 2) Access, page 10-7
- Network Operator (Level 3) Access, page 10-7
- Network Administrator (Level 4) Access, page 10-7
- System Administrator (Level 5) Access, page 10-8

The authentication level that includes a function is the *lowest* level with access to that function. The function is also available to all higher authentication levels. For example, a System Administrator also has access to all Network Administrator functions.

Authentication levels are based on the function to be performed, not on the target object. Therefore, if a user can perform a function on one MWTM object (such as deleting a node), the user can perform the same function on all similar MWTM objects.

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

To configure the authentication level for a user, use the **mwtm adduser** command, as described in the "Implementing MWTM User-Based Access (Server Only)" section on page 10-2, or the **mwtm updateuser** or **mwtm newlevel** command, as described in the "Enabling and Changing Users and Passwords (Server Only)" section on page 10-13.

Basic User (Level 1) Access

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

Basic Users have access to the following MWTM functions:

- Connecting to a new server
- Applying changes to views
- Loading the DEFAULT view and existing views, but not saving them
- Editing, loading, and applying preferences files, but not saving them
- Viewing and manipulating the topology map, and saving it as a JPEG, but not saving icon locations
- Viewing network objects, events, details, and notes
- Viewing the MWTM home page
- Loading existing event filters, but not saving them
- Printing MWTM windows
- Launching CiscoWorks

Basic Users have access to the following MWTM Web displays:

- Server Home Page
- System README
- Network Status

- System Data Files
  - Notes
  - Views
  - Preferences
- Viewing MWTM documentation
- Downloading client software

Power User (Level 2) Access

Power Users have access to all Basic User functions.

Power Users can change some aspects of the way MWTM works.

Power Users have access to the following MWTM functions:

- Editing network objects, events, and views
- Unignoring network objects and views
- Saving preferences files, event filters, and views
- Acknowledging events
- Viewing MWR real-time data and charts
- Viewing the event configuration, but not editing it

Power Users have access to the following MWTM Web displays:

- System Status, excluding User Accounts and System Troubleshooting
- Network Statistics Reports

Network Operator (Level 3) Access

Network Operators have access to all Basic User and Power User functions.

Network Operators can make changes to MWTM network files.

Network Operators have access to the following MWTM functions:

- Ignoring network objects and views
- Polling nodes
- Telnetting to the MWR

Network Administrator (Level 4) Access

Network Administrators have access to all Basic User, Power User, and Network Operator functions.

Network Administrators have access to all MWTM client functions.

Network Administrators have access to the following MWTM functions:

- SNMP configuration
- Network Discovery
- Deleting network objects
- Managing and unmanaging nodes

- Using the Deployment Wizard

Network Administrators have access to the following MWTM Web displays:

- System Data Files: Discovery Seeds

System Administrator (Level 5) Access

System Administrators have access to all Basic User, Power User, Network Operator, and Network Administrator functions.

System Administrators have access to all functions in MWTM.

System Administrators have access to the following MWTM Web displays:

- System Messages and Logs
- System Status, including User Accounts and System Troubleshooting
- Trap Configuration, including SNMP configuration information
- System Information
  - System Command Log
  - System Console Log
  - System Event Automation Log
  - System Install Log
  - System Process Services
  - System Properties
  - System Root Variables
  - System Security Log
  - System Web Access Log
  - System Web Error Log

Automatically Disabling Users and Passwords (Server Only)

After you have implemented the basic MWTM User-Based Access security system, you can customize the system to automatically disable users and passwords when certain conditions are met.

To automatically disable users and passwords, use the following procedures:

Step 1 Log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, or as a super user, as described in the "Specifying a Super User (Server Only)" section on page 10-19.

Step 2 Enter the following command:

# cd /opt/CSCOsgm/bin

Step 3 (Optional) You can configure MWTM to generate an alarm after a specified number of unsuccessful login attempts by a user. To do so, enter the following command:

# ./mwtm badloginalarm *number-of-attempts* where *number-of-attempts* is the number of unsuccessful login attempts allowed before 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 function (that is, to prevent MWTM from automatically generating an alarm after unsuccessful login attempts), enter the following command:

# ./mwtm badloginalarm clear

Step 4 (Optional) You can configure MWTM to disable a user's security authentication automatically after a specified number of unsuccessful login attempts. To do so, enter the following command:

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

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

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 authentication, use the **mwtm enableuser** command.

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

# ./mwtm badlogindisable clear

Step 5 (Optional) MWTM keeps track of the date and time each user last logged in. You can configure MWTM to disable a user's security authentication automatically after a specified number of days of inactivity. To do so, enter the following command:

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

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

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

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

This function 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 function and you want to disable it (that is, to prevent MWTM from automatically disabling user accounts as a result of inactivity), enter the following command:

# ./mwtm inactiveuserdays clear

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

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

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

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

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

This function 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 function and you want to disable it (that is, prevent MWTM from forcing users to change passwords), enter the following command:

```
# ./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) You can configure MWTM to disconnect an MWTM client automatically after a specified number of minutes of inactivity. To do so, enter the following command:

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

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

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

This function 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 function 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)" section on page 10-8, you can customize MWTM to automatically disable users and passwords when certain conditions are met. However, you can also manually disable MWTM User-Based Access users and passwords when the need arises. To do so, use the following procedures:

Step 1 Log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, or as a super user, as described in the "Specifying a Super User (Server Only)" section on page 10-19.

Step 2 Enter the following command:

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

Step 3 (Optional) To delete a user entirely from the MWTM User-Based Access authentication list, enter the following command:

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

where *username* is the name of the user.

If you later decide to add the user back to the authentication 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 do so, enter the following command:

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

where *username* is the name of the user. MWTM does not delete the user from the authentication list, 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 his password the next time he logs in.

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

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

Step 5 (Optional) To disable a user's authentication, but not the user's password, use the following command:

```
# ./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 super user, to enter this command.

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

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

Enabling and Changing Users and Passwords (Server Only)

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

Step 1 Log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, or as a super user, as described in the "Specifying a Super User (Server Only)" section on page 10-19.

Step 2 Enter the following command:

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

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

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

where *username* is the name of the user. MWTM re-enables the user's authentication 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 super user, 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 authentication with a new password, if the user's authentication had been disabled either automatically by MWTM or by a super user. To change a password or to re-enable a user's authentication with a new password, enter the following command:

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

where *username* is the name of the user.

MWTM prompts you for the new password. When setting the password, follow the rules and considerations in the "Creating Secure Passwords" section on page 10-5.

If the user's authentication has also been disabled, MWTM re-enables the user's authentication 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 authentication 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 super user, to enter this command.

MWTM prompts you for the new authentication level. Valid levels are:

- **1**—Basic User

- **2**—Power User
- **3**—Network Operator
- **4**—Network Administrator
- **5**—System Administrator

For more information about authentication levels, see the "Configuring MWTM User Authentication Levels (Server Only)" section on page 10-6.

If **mwtm authtype** is set to **local**, MWTM also prompts you for the user's new password. When setting the password, follow the rules and considerations in the "Creating Secure Passwords" section on page 10-5.

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

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

where *username* is the name of the user.

MWTM prompts you for the new authentication level. Valid levels are:

- **1**—Basic User
- **2**—Power User
- **3**—Network Operator
- **4**—Network Administrator
- **5**—System Administrator

For more information about authentication levels, see the “Configuring MWTM User Authentication Levels (Server Only)” section on page 10-6.

Displaying a Message of the Day (Server Only)

MWTM enables you 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 before launching.

If the message of the day is enabled, it is displayed whenever a user attempts to launch an MWTM 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 the MWTM client. If there is a message of the day, the Message of the Day dialog is displayed.
- Select **View > Message of the Day** from the MWTM Main Menu.

- Select the MWTM server name in the bottom right corner of the MWTM Main Window.
- MWTM displays the Message of the Day dialog

The Message of the Day dialog contains the following fields and buttons:

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, MWTM displays **Unknown**.
Message Field	Text of the message of the day. If there is no message of the day, 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 the MWTM 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 the MWTM 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 selecting **View > Message of the Day** from the MWTM Main Menu.

If you want to configure MWTM to display a message of the day, you must first enable the function. To do so, log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, or as a super user, as described in the "Specifying a Super User (Server Only)" section on page 10-19, then enter the following commands:

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

```
# ./mwtm motd enable
```

MWTM displays the following prompt:

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

To accept the default value, press **Enter**; or type a different location and press **Enter**. MWTM displays the following messages:

```
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.
```

Initially, the file is blank; enter the following command to specify the message text:

```
# ./mwtm motd edit
```

You can also use the **mwtm motd edit** command at any time to change the text of the message of the day.

To display the contents of the message of the day file, enter the following command:

```
# ./mwtm motd cat
```

To disable this function (that is, to stop displaying the message of the day whenever a user attempts to launch an MWTM client), enter the following command:

```
# ./mwtm motd disable
```

Manually Synchronizing Local MWTM Passwords (Server Only)

If **mwtm authtype** is set to **solaris** or **linux**, MWTM automatically synchronizes local MWTM passwords with the operating system at 1:30 AM each night. However, you can also manually synchronize passwords at any time. To do so, log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, then enter the following commands:

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

```
# ./mwtm syncusers
```

MWTM synchronizes the passwords with Solaris.

Listing All Currently Defined Users (Server Only)

You can list all currently defined users in the MWTM User-Based Access authentication list. To do so, log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, or as a super user, as described in the "Specifying a Super User (Server Only)" section on page 10-19, then enter the following commands:

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

```
# ./mwtm listusers
```

MWTM displays the following information for each user:

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

To list information for only a specific user, enter the following command:

```
# ./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. For more information, see the "Viewing MWTM User Account Information" section on page 13-44.

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

You can display the contents of the system security log with PAGER. To do so, log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, or as a super user, as described in the "Specifying a Super User (Server Only)" section on page 10-19, then enter the following commands:

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

```
# ./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 authentication 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

To clear the log and restart the server, enter the following command:

```
# ./mwtm seclog clear
```

The default path and filename for the system security log file is */opt/CSCOsgm/logs/sgmSecurityLog.txt*. If you installed 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 the "Viewing the MWTM System Security Log" section on page 13-41.

Restoring Security-Related MWTM Data (Server Only)

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

To restore the files, log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, then enter the following commands:

```
# cd /opt/CSCOsgm/bin

# ./mwtm restore security
```

mwtm restores the files.

Disabling MWTM User-Based Access (Server Only)

For some reason, you might want to completely disable MWTM User-Based Access. To do so, log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, or as a super user, as described in the "Specifying a Super User (Server Only)" section on page 10-19, then enter the following commands:

```
# cd /opt/CSCOsgm/bin

# ./mwtm useraccess disable
```

MWTM User-Based Access is disabled the next time you restart the MWTM server, using the following command:

```
# ./mwtm restart
```

Specifying a Super User (Server Only)

MWTM enables you to specify one or more *super users*. A super user can perform most functions that otherwise require the user to be logged in as the root user. (The root user can still perform those functions, too.) If you specify a super user, the server also runs as the super user and not as the root user.

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

To specify a super user, log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, then enter the following commands:

```
# cd /opt/CSCOsgm/bin

# ./mwtm superuser username
```

where *username* is the name of the user.

When you specify a super user, keep in mind the following considerations:

- 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 super user does not have access to all MWTM commands. You must still be logged in as the root user to enter the following commands:
  - **mwtm backup**
  - **mwtm browserpath**
  - **mwtm certgui**
  - **mwtm certtool**
  - **mwtm clean**
  - **mwtm cleanall**
  - **mwtm cleandb**
  - **mwtm cw2ksetup**
  - **mwtm evilstop**
  - **mwtm jspport**
  - **mwtm keytool**
  - **mwtm killclients**
  - **mwtm reboot**
  - **mwtm restore**
  - **mwtm restoreprops**
  - **mwtm setpath**, if you are specifying a *username*
  - **mwtm ssl**
  - **mwtm sslstatus**
  - **mwtm stopclients**
  - **mwtm superuser**
  - **mwtm syncusers**
  - **mwtm telnetpath**
  - **mwtm trapsetup**
  - **mwtm uninstall**

  - **mwtm webport**
  - **mwtm xtermpath**
- If **mwtm authtype** is set to **solaris**, you must still be logged in as the root user to enter the following commands:
  - **mwtm adduser**
  - **mwtm disableuser**
  - **mwtm enableuser**
  - **mwtm updateuser**
- 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 RAN-O devices in your network, use the **snmp-server host** command. By default, MWTM listens for traps from trap multiplexing devices 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 RAN-O devices in your network.
  - See the description of the **snmp-server host** command in the "RAN-O Requirements" section of the *Cisco Signaling Gateway Manager Installation Guide* for more information.
  - Use the **mwtm trapsetup** command to change the SNMP trap port number in the MWTM server to match the port number in the RAN-O devices in your network. See the "mwtm trapsetup" section on page C-69 for more information.

Implementing SSL Support in MWTM (Solaris Only)

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

This section includes the following information:

- Enabling SSL Support in MWTM, page 10-22
- Downloading the MWTM Server's Self-Signed SSL Certificate, page 10-24
- Launching the MWTM Certificate Tool for SSL, page 10-26
- Importing an SSL Certificate to an MWTM Client, page 10-26
- Exporting an SSL Certificate, page 10-28
- Viewing Detailed Information About an SSL Certificate, page 10-29
- Managing SSL Support in MWTM, page 10-30
- Disabling SSL Support in MWTM, page 10-32

Enabling SSL Support in MWTM

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

Step 1 Obtain the SSL-enabled version of MWTM.

Due to US government restrictions on the export of SSL-enabled software, Cisco provides two versions of MWTM: Basic MWTM, which does not provide SSL support, and SSL-enabled MWTM, which does.

To obtain SSL-enabled MWTM, you must contact Cisco TAC or your Cisco Account Team. They will help you apply for an export licence and download and install SSL-enabled MWTM.

Step 2 Install an SSL key/certificate pair in MWTM, 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.

  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 []:
  ```

  Enter the requested information.

  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.cer* 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 CA-signed certificate, generate the key and a CSR by logging in as the root user on the MWTM server and entering the **mwtm keytool genkey** command.

  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 []:
  ```

  Enter the requested information.

  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.cer* 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 certificate authority (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.

  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.

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

Step 3 Enable SSL support in MWTM, by logging in as the root user on the MWTM server and entering the **mwtm ssl enable** command.

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.cer*), using the procedure in the "Downloading the MWTM Server's Self-Signed SSL Certificate" section on page 10-24.

b. Import the self-signed or CA-signed certificate, using the procedure in the "Importing an SSL Certificate to an MWTM Client" section on page 10-26.

Step 5 Restart the MWTM client.

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

If an MWTM client that is not SSL-enabled attempts to connect to an SSL-enabled MWTM server, MWTM displays an appropriate warning message and opens the MWTM client download page. The user can then download and install a new MWTM client to use to connect to that MWTM server.

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

Downloading the MWTM Server's Self-Signed SSL Certificate

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 Use one of the following procedures to access the MWTM Server Home Page:

- Select **View > MWTM Server > Home Page** from the MWTM Main Menu.
- Enter the following URL in a Web browser:

  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 MWTM. (**1774** is the default port number.) If you do not know the name or Web port of the MWTM Web Server, contact the system administrator who installed the MWTM server software.

MWTM displays the MWTM Server Home page.

Step 2 Select **Server SSL Certificate** from the MWTM Server Home Page. MWTM displays the MWTM Server SSL Certificate page.

Step 3 Right-click **Download MWTM Server SSL Certificate**.

Step 4 Select **Save Link As** from the right-click menu.

Step 5 Select a directory in which to save the certificate (*server.cer*), and click **Save**. MWTM downloads the *server.cer* 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 lists all SSL certificates that have been imported by the MWTM client, and enables you 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
  ```

  See the "mwtm certgui" section on page C-9 for more information.

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

MWTM displays the MWTM Certificate Tool dialog

The MWTM Certificate Tool dialog displays the following information about each SSL certificate:

Field or Button	Description
Issued to	Host name 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 host name of the MWTM server.
Expiration Date	Date on which the SSL certificate expires.
Import	Displays the Open dialog for an SSL certificate, which enables you to import SSL certificates.
Export	Displays the Save dialog for an SSL certificate, which enables you to export the selected SSL certificate.
Remove	Removes the selected SSL certificate from the table.
Details	Displays the Certificate Information dialog, which provides detailed information about the selected certificate.
Exit	Closes the MWTM Certificate Tool dialog.
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.

To import an SSL certificate, launch the MWTM SSL Certificate Tool, as described in the "Launching the MWTM Certificate Tool for SSL" section on page 10-26, then click **Import**. MWTM displays the Open dialog for SSL certificates

Use the Open dialog to locate the SSL certificate that you want to import. The Open dialog for an SSL certificate provides the following fields and buttons:

Field or Button	Description
Look In	Enables you to select the directory in which you want to find the SSL certificate. Either 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. 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 are displayed in the table.
Up One Level	Displays the sub-folders and files that are in the folder that is up one level from the currently displayed folder.
Desktop	Displays the sub-folders and files that are on your workstation desktop.
Create New Folder	Creates a new sub-folder in the displayed folder.
List	Displays only icons for sub-folders and files.
Details	Displays detailed information for sub-folders and files, including their size, type, date they were last modified, and so on.
Open	Imports the file, closes the Open dialog for an SSL certificate, and populates the MWTM Certificate Tool dialog with the SSL certificate's information.
Cancel	Closes the Open dialog for an SSL certificate without importing the file.

Related Topics:

- Launching the MWTM Certificate Tool for SSL, page 10-26

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 an SSL certificate, launch the MWTM SSL Certificate Tool, as described in the "Launching the MWTM Certificate Tool for SSL" section on page 10-26, select a certificate from the list, then click **Export**. MWTM displays the Save dialog for SSL certificates

Use the Save dialog to export the SSL certificate to another directory. The Save dialog for an SSL certificate provides the fields and buttons:

Field or Button	Description
Save In	Enables you to select the directory in which you want to save the SSL certificate. Either 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. 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 are displayed in the table.
Up One Level	Displays the sub-folders and files that are in the folder that is up one level from the currently displayed folder.
Desktop	Displays the sub-folders and files that are on your workstation desktop.
Create New Folder	Creates a new sub-folder in the displayed folder.
List	Displays only icons for sub-folders and files.
Details	Displays detailed information for sub-folders and files, including their size, type, date they were last modified, and so on.
Save	Saves the file, closes the Save dialog for an SSL certificate, and returns to the MWTM Certificate Tool dialog. Click **Exit** to close the MWTM Certificate Tool dialog 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 10-26

Viewing Detailed Information About an SSL Certificate

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

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

- Click the “locked padlock” symbol in the bottom left corner of any MWTM window.
- Launch the MWTM SSL Certificate Tool, as described in the “Launching the MWTM Certificate Tool for SSL” section on page 10-26, select an SSL certificate from the list and click **Details**.

MWTM displays the Certificate Information dialog

The Certificate Information dialog displays the following detailed information for the selected SSL certificate:

Field or Button	Description
Subject	Device to which the SSL certificate was issued. The **Subject** field always includes the Common Name (CN) of the subject, which must match the fully qualified host name of your MWTM server, such as **mwtm-sun8.cisco.com**. The **Subject** 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. The **Issuer** 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 used to ensure 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. When you are ready to close the dialog, click **OK**. MWTM closes the Certificate Information dialog. If necessary, click **Exit** to close the MWTM Certificate Tool dialog.

Related Topics:

- Launching the MWTM Certificate Tool for SSL, page 10-26

Managing SSL Support in MWTM

MWTM enables you to perform the following tasks to make it easier to manage SSL support in MWTM:

- To display the current status of SSL support in 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.
- To print the MWTM server's SSL certificate in X.509 format, use the **mwtm keytool print_crt** command.
- To list the SSL key/certificate pair on the MWTM server, use the **mwtm keytool list** command.
- To list all SSL certificates on the MWTM client, launch the MWTM SSL Certificate Tool. MWTM lists each imported certificate, including to whom the certificate was issued, who issued the certificate, and when the certificate expires.

See the "MWTM Command Reference" section on page C-1 for more information on the use of these commands.

See the "Importing an SSL Certificate to an MWTM Client" section on page 10-26 for more information on launching the MWTM SSL Certificate Tool.

Disabling SSL Support in MWTM

MWTM enables you to disable SSL support in MWTM, and to remove SSL keys and certificates from the MWTM server and clients:

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

  See the "mwtm ssl" section on page C-57 for more information.

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

  See the "MWTM Command Reference" section on page C-1 for more information on the use of these commands.

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

  See the "Importing an SSL Certificate to an MWTM Client" section on page 10-26 for more information on launching the MWTM SSL Certificate Tool.

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

By default, when you first install MWTM, all MWTM client IP addresses are allowed to connect to the MWTM server. However, MWTM enables you 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. MWTM allows connections from only those clients, plus the local host. If the file exists but is empty, MWTM allows connections only from the local host. (MWTM always allows connections from the local host.)

When you first install MWTM, the *ipaccess.conf* file does not exist and 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, use the following procedure:

Step 1 Log in as the root user, as described in the "Becoming the Root User (Server Only)" section on page 3-3, or as a super user, as described in the "Specifying a Super User (Server Only)" section on page 10-19.

Step 2 Enter the following command:

```
# 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 the following command:

  ```
  # ./mwtm ipaccess add
  ```

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

```
# ./mwtm ipaccess edit
```

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

- If you installed MWTM in the default directory, */opt*, then the default directory is */opt/CSCOsgm/etc*.
- If you installed 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, the address *.*.*.* allows all clients to connect to the MWTM server.

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.

See the "mwtm ipaccess" section on page C-23 for more information.

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

MWTM also enables you 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 (Server Only)" section on page 11-29.