CHAPTER 3

Setting Up Your Server

This chapter contains:

Importing SNMP Community Names from CiscoWorks (Solaris Only)

You can use the Cisco Mobile Wireless Transport Manager (MWTM) to store all SNMP community names in a single database in CiscoWorks Common Services (CS), and to export those names for use by the MWTM.

To export the database from CiscoWorks CS to the MWTM:

Step 1 Log in to CiscoWorks. From the Common Services tab, choose **Device and Credentials > Device Management**.

Step 2 Click the **Export** button.

Step 3 In the tree in the left pane, select the device(s) for export. To choose all devices, click the box next to CS@<*your_server_name*>. To choose an individual device:

- Expand the hierarchy
- Drill-down to find an individual device
- Click the box next to the corresponding device

Step 4 In the fields in the right pane, enter:

```
File Name = mwtm
Format = CSV
```

CiscoWorks creates the *mwtm* file in the default export directory, */opt/CSCOpx/objects/dmgt*. When you start the MWTM server, the MWTM looks for this file. If the file exists, the MWTM merges the file with its own community name database, and the exported SNMP community names will appear in the SNMP tab of the Node SNMP and Credentials dialog box (see Configuring Nodes, page 3-14.)

Tip For more information about SNMP, refer to "Configuring SNMP Support" in the Cisco IOS Release 12.2 *Configuration Fundamentals Configuration Guide*, Part 3, System Management.

Changing MWTM Server Poller Settings

Note For details on changing poller settings using the MWTM client or MWTM web interface, see Changing Client and Web Preference Settings, page 5-1

The MWTM provides four pollers for use in the MWTM client GUI and web pages: a fast poller, a slow poller, a status refresh poller, and a memory poller. Using the MWTM, you can change the settings (such as minimum, maximum, and default) for each poller. However, the only setting you can modify for the memory poller is the timeout value.

To change server poller settings:

Step 1 Edit the *Server.properties* file:

- If you installed the MWTM in the default directory, */opt*, then the location of the *Server.properties* file is */opt/CSCOsgm/properties/Server.properties*.
- If you installed the MWTM in a different directory, then the *Server.properties* file is located in that directory.

Step 2 To change fast poller settings, change one or more of these lines in the file:

```
# Fast poller default polling interval in seconds
FAST_POLLER_DEFAULT = 15

# Fast poller minimum polling interval in seconds
FAST_POLLER_MIN = 5

# Fast poller maximum polling interval in seconds
FAST_POLLER_MAX = 60
```

For example, to change the fast poller default to 30 seconds, change the FAST_POLLER_ DEFAULT line to:

```
FAST_POLLER_DEFAULT = 30
```

Step 3 To change slow poller settings, change one or more of these lines in the file:

```
# Slow poller default polling interval in seconds
SLOW_POLLER_DEFAULT = 60

# Slow poller minimum polling interval in seconds
SLOW_POLLER_MIN = 60

# Slow poller maximum polling interval in seconds
SLOW_POLLER_MAX = 300
```

For example, to change the slow poller default to 180 seconds, change the SLOW_POLLER_DEFAULT line to:

```
SLOW_POLLER_DEFAULT = 180
```

Step 4 To change status refresh poller settings, change one or more of these lines in the file:

```
# Status refresh default interval in seconds
STATE_REFRESH_DEFAULT = 180

# Status refresh minimum interval in seconds
STATE_REFRESH_MIN = 180

# Status refresh maximum interval in seconds
STATE_REFRESH_MAX = 900
```

For example, to change the status refresh poller default to 300 seconds, change the STATE_REFRESH_DEFAULT line to:

```
STATE_REFRESH_DEFAULT = 300
```

Step 5 To change memory poller settings, update the following value:

```
MEMORY_POLLER_TIMEOUT_INCREMENT = 5000
```

Step 6 Save your changes and restart the MWTM server.

Any changes you make take effect when you restart the MWTM server, and are reflected throughout the MWTM client GUI and web pages at that time.

For each of these pollers, remember that, if you set the:

- Minimum interval for a poller to less than 0 seconds, the MWTM overrides that setting and resets the minimum interval to 0 seconds.
- Maximum interval for a poller to less than the minimum interval, the MWTM overrides that setting and resets the maximum interval to be equal to the minimum interval.
- Default interval for a poller to less than the minimum interval, the MWTM overrides that setting and resets the default interval to be equal to the minimum interval.
- Default interval for a poller to more than the maximum interval, the MWTM overrides that setting and resets the default interval to be equal to the maximum interval.

Tip Due to potential timeouts during memory polling, Cisco does not recommend that you set the memory timeout add-on value to anything less than the default of 5000 milliseconds. If the MWTM encounters memory timeouts during normal day-to-day operations, you can increment this value to alleviate the problem.

Changing the Message Display

These sections contain information about changing the way the MWTM displays and stores messages:

Changing the Location of MWTM Message Log Files

By default, all MWTM system message log files are located on the MWTM server at */opt/CSCOsgm/logs*. To change the location of the system message log directory, use the **mwtm msglogdir** command. For more information, see mwtm msglogdir, page B-46.

Changing the Size of the MWTM Message Log Files

To change the size of the message log files, use the **mwtm logsize** command. For more information, see mwtm logsize, page B-39.

Changing the Time Mode for Dates in Log Files

To change the time mode for dates in log files, use the mwtm logtimemode command. For more information, see mwtm logtimemode, page B-40.

Changing the Age of the MWTM Message Log Files

To change the number of days the MWTM archives system message log files before deleting them from the MWTM server, use the **mwtm msglogage** command. For more information, see mwtm msglogage, page B-45.

Setting the ITP Point Code Format

You can use the MWTM to set a new point code format for an MWTM server. The MWTM server and all associated MWTM clients use the new point code format. Normally, you need to do this only once, after installation.

Note When setting the ITP Point Code Format, if a discovery has already occurred, some node and signaling point objects will have been named using the old format. These names will not be affected by the new format. To force the objects to be recreated using the new point code format, you must perform an **mwtm cleandb**.

After you perform the **mwtm cleandb**, the network will need to be discovered again to populate the device names based on the new signaling point format.

The point code format configuration is contained in the *PointCodeFormat.xml* file.

To set the new point code format, log in as the root user, as described in Starting the MWTM Client, page 4-2, or as a superuser, as described in Specifying a Super User (Server Only), page 2-20. Then enter:

```
# cd /opt/CSCOsgm/bin
# ./mwtm pcformat [edit | list | master | restore]
```

Where:

- edit—Opens the *PointCodeFormat.xml* file for editing, using $EDITOR environment variable if set, otherwise uses vi.
- list—Displays the current contents of the *PointCodeFormat.xml* file.
- master—Restores the *PointCodeFormat.xml* file to the default settings.
- restore—Restores the *PointCodeFormat.xml* file to the last saved copy.

The *PointCodeFormat.xml* file provides these default point code formats:

- <Variant value="ANSI" format="8.8.8"/>—Formats point codes using the 24-bit American National Standards Institute (ANSI) standard format, *xxx.yyy.zzz*, where:
  - *xxx* is the 8-bit network identification
  - *yyy* is the 8-bit network cluster
  - *zzz* is the 8-bit network cluster member

- <Variant value="China" format="8.8.8"/>—Formats point codes using the 24-bit China standard format, *xxx.yyy.zzz*, where:
  - *xxx* is the 8-bit network identification
  - *yyy* is the 8-bit network cluster
  - *zzz* is the 8-bit network cluster member
- <Variant value="ITU" format="3.8.3"/>—Formats point codes using the 14-bit International Telecommunication Union (ITU) standard format, *x.yyy.z*, where:
  - *x* is the 3-bit zone identification
  - *yyy* is the 8-bit region identification
  - *z* is the 3-bit signal-point
- <Variant value="NTT" format="5.4.7" readBits=”rightToLeft”/>— Formats point codes using the 16-bit Nippon Telegraph and Telephone Corporation (NTT) standard format, *xx.yy.zzz*, where:
  - *xx* is the 5-bit zone identification
  - *yy* is the 4-bit area/network identification
  - *zzz* is the 7-bit identifier
- <Variant value="TTC" format="5.4.7" readBits=”rightToLeft”/>— Formats point codes using the 16-bit Telecommunication Technology Committee (TTC) standard format, *xx.yy.zzz*, where:
  - *xx* is the 5-bit zone identification
  - *yy* is the 4-bit area/network identification
  - *zzz* is the 7-bit identifier

As shown previously, the standard point code format for each variant is three octets. (For example, 3.8.3 for ITU.) However, you can also specify a four-octet format for any of the variants. (For example, 4.3.4.3 for ITU.) The total number of bits must still equal 24 for ANSI and China, 14 for ITU, and 16 for NTT and TTC.

For information about customizing the point code formats, including setting a new three-octet or four-octet format, see the detailed instructions in the *PointCodeFormat.xml* file.

Any changes that you make take effect when you restart the MWTM server.

The MWTM preserves customized point code formats when you upgrade to a new version or release of the MWTM.

Connecting a Single-Instance ITP to a Multiple-Instance ITP

You can configure the MWTM to recognize a single-instance ITP connecting to multiple instances on a multiple-instance ITP. In effect, the MWTM views the multiple networks as a single all-encompassing network.

To connect single-instance ITPs to multiple-instance ITPs:

Step 1 Log in as the root user, as described in Starting the MWTM Client, page 4-2, or as a superuser, as described in Specifying a Super User (Server Only), page 2-20.

Step 2 Enter:

```
# cd /opt/CSCOsgm/bin
# ./mwtm pcformat edit
```

The mwtm pcformat edit command opens the *PointCodeFormat.xml* file for editing. For more information about using this command, see Setting the ITP Point Code Format, page 3-5.

Step 3 Add these lines to the *PointCodeFormat.xml* file:

```
<NetworkConfig>
    <Network value="Big-Network">
        <Include value="Network-1"/>
        <Include value="Network-2"/>
        <Include value="Network-3"/>
    </Network>
</NetworkConfig>
```

Where:

- *Network-1*, *Network-2*, and *Network-3* are the names of your subnetworks. (This example assumes that you are combining three subnetworks into one.)
- *Big-Network* is the name of the combined network that includes *Network-1*, *Network-2*, and *Network-3*.

  In the MWTM, the signaling point Instance Name field displays the subnetwork name (for example, Network-1), and the Point Code field displays the name of the combined network (for example, Big-Network).

  During Discovery, the MWTM assigns a default name to each discovered signaling point. The assigned default name consists of the point code and the combined network name (for example, 3.8.3:Big-Network).

Step 4 Save your changes to the *PointCodeFormat.xml* file.

Step 5 Restart the MWTM server. Any changes you made to the *PointCodeFormat.xml* file take effect when you restart the MWTM server.

The MWTM preserves the customized network configuration when you upgrade to a new version or release of the MWTM.

Enabling SNMP Traps

By default, the MWTM cannot receive SNMP traps. To use SNMP traps with the MWTM, you must first configure the MWTM to receive traps.

Related Topics:

Integrating the MWTM with Other Products, page 5-39

To view the current trap reception configuration for the MWTM:

Step 1 Log in as the root user, as described in Starting the MWTM Client, page 4-2, or as a superuser, as described in Specifying a Super User (Server Only), page 2-20.

Step 2 Enter:

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

The MWTM displays the current trap reception configuration for the MWTM, including:

- Whether receiving traps is enabled or disabled
- Which UDP port the MWTM trap receiver is listening on

To configure the MWTM to receive traps:

Step 1 Log in as the root user, as described in Starting the MWTM Client, page 4-2, or as a superuser, as described in Specifying a Super User (Server Only), page 2-20.

Step 2 Enter:

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

The MWTM displays:

```
The MWTM server must also be stopped to perform this operation.
Do you wish to continue? [n]
```

Step 3 Type **y** and press **Enter**. The MWTM stops the MWTM Process Manager and all managed processes and displays:

```
Would you like to configure MWTM to receive SNMP traps? [yes]
```

Step 4 Press **Enter**. The MWTM displays:

```
MWTM can receive traps natively on the standard UDP port number 162
or on any other UDP port chosen. If another application is already
bound to the SNMP standard trap reception port of 162, an alternate
port number for MWTM to receive traps must be specified.

UDP port number 44750 is the default alternate port.

Enter trap port number? [ 162 ]
```

Step 5 By default, nodes send traps to port 162. To accept the default value, press **Enter**.

Step 6 If your nodes have been configured to send traps to a different port, type that port number and press **Enter**.

Step 7 By default, the MWTM listens for traps from trap-multiplexing nodes and NMS applications on port 44750. If you want the MWTM to monitor that port, and port 162 is not available on the MWTM server host, type **44750** and press **Enter**.

Step 8 If trap multiplexing nodes and NMS applications in your network have been configured to send traps to a different port, type that port number and press **Enter**.

Step 9 If you are a superuser, you must specify a port number that is greater than 1024, then press **Enter**.

Do not enter a non numeric port number. If you do, you are prompted to enter a numeric port number.

When you select an SNMP trap port number for the MWTM server, ensure your nodes use the same SNMP trap port number. See the description of the snmp-server host command in the "Preparing to Install the MWTM" chapter of the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1* for more information.

Step 10 To accept the default value, press **Enter**; or, type a different location and press **Enter**.

The MWTM confirms your choices and restarts the MWTM Process Manager and all managed processes.

You can change all aspects of MWTM event processing, including the size of the MWTM event database, the maximum length of time the MWTM is to retain events, and the default severity and color associated with each type of event. If a new trap becomes available that is of interest to the MWTM, you can add it to the MWTM event database, enabling the MWTM to recognize and process the new trap. For more information about changing MWTM event processing, see Changing the Way the MWTM Processes Events, page 9-35.

Limiting Traps by IP Address

By default, when you first install the MWTM, all IP addresses are allowed to send traps to the MWTM server. However, you can use the MWTM to limit the IP addresses that can send traps to the server by creating and maintaining the *trapaccess.conf* file.

You can create the *trapaccess.conf* file and populate it with a list of IP addresses that can send traps to the MWTM server. The MWTM receives traps from only those IP addresses, plus the local host. If the file exists but is empty, the MWTM receives traps only from the local host. (The MWTM always receives traps from the local host.)

When you first install the MWTM, the *trapaccess.conf* file does not exist and the MWTM allows all IP addresses to send traps to the MWTM server.

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

Step 1 Log in as the root user, as described in Starting the MWTM Client, page 4-2, or as a superuser, as described in Specifying a Super User (Server Only), page 2-20.

Step 2 Enter:

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

Step 3 Create the *trapaccess.conf* file:

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

```
# ./mwtm trapaccess add

   Enter address to add: 1.2.3.4
   IP Address 1.2.3.4 added.
   MWTM server must be restarted for changes to take effect.
   Use the following command to restart the server:
      mwtm restart
```

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

```
# ./mwtm trapaccess 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*.
- In a different directory, then the default directory resides in that directory.

In the *trapaccess.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 send traps to the MWTM server.

After you create the *trapaccess.conf* file, you can use the full set of mwtm trapaccess keywords to work with the file. For more details, see mwtm trapaccess, page B-75.

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

Configuring a Backup MWTM Server

You can use the MWTM to configure a second MWTM server as a backup for the primary MWTM server. For best results, Cisco recommends that you configure the primary server and the backup server as backups for each other.

To configure a backup MWTM server:

Step 1 Log in as the root user, as described in Starting the MWTM Client, page 4-2, or as a superuser, as described in Specifying a Super User (Server Only), page 2-20.

Step 2 Enter:

```
# cd /opt/CSCOsgm/bin
# ./mwtm secondaryserver hostname naming-port webport
```

where:

- *hostname* is the optional name of the host on which the backup MWTM server is installed.
- *naming-port* is the optional MWTM Naming Server port number for the backup MWTM server. The default port number is 44742.
- *webport* is the optional MWTM web port number for the backup MWTM server. The default port number is 1774.

Note If you use the mwtm secondaryserver command to configure a backup MWTM server, but the primary MWTM server fails before you launch the MWTM client, then the MWTM client has no knowledge of the backup server.

Step 3 (Optional) To list the backup MWTM server that has been configured for this primary MWTM server, enter:

```
# cd /opt/CSCOsgm/bin
# ./mwtm secondaryserver list
```

Step 4 (Optional) To configure whether or not a prompt appears on the client in the event of server failover, see mwtm clientfailoverprompt, page B-17.

Configuring an MWTM Client Connection Timer

You can use the MWTM to specify how long an MWTM client is to wait for the MWTM server before exiting.

To configure an MWTM client connection timer:

Step 1 Login as the root user, as described in Starting the MWTM Client, page 4-2, or as a superuser, as described in Specifying a Super User (Server Only), page 2-20.

Step 2 Enter:

```
# cd /opt/CSCOsgm/bin
# ./mwtm cliconntimer number-of-seconds
```

where *number-of-seconds* is the time the MWTM client is to wait for a message from the MWTM server before exiting. The valid range is 10 seconds to an unlimited number of seconds. The default value is 60 seconds.

If the timer expires, the client attempts to contact the server and takes one of these actions. If the server:

- Responds to the client, the client reconnects to the server.
- Does not respond to the client, but a backup server is configured, the client attempts to connect to the backup server.
- Does not respond to the client, and no backup server is configured, the client displays a dialog box with this message:

  ```
  Connection to the server has timed out.
  Client could not establish 2-way communications with the server.
  If you are running through a VPN you may have entered the wrong client IP address.
  ```

  Click **OK** to exit the client. The MWTM writes this message to the client console log:

  - Solaris or Linux client—*/opt/CSCOsgmClient/logs/sgmConsoleLog.txt*
  - Windows client—*C:\Program Files\Cisco Systems\MWTM Client\logs\consoleLog.txt*

The timer takes effect when you restart the MWTM server.

Step 3 (Optional) To restore the default timeout of 60 seconds, enter:

```
# ./mwtm cliconntimer clear
```

The timer is reset to 60 seconds when you restart the MWTM server.

Enabling the Terminal Server Proxy Service

The MWTM provides the capability to function through firewalls, where the server is located behind the firewall and the client is outside the firewall. To use this feature, enable the terminal proxy service by the mwtm termproxy command (see mwtm termproxy, page B-75).

Setting Up TFTP on Your Server (ITP Only)

Before deploying or loading route table, GTT, or MLR address table files, the TFTP daemon must be running on the Solaris or Linux server.

Tip For more information about questions regarding TFTP, see When I try to deploy routes, GTT files, or address table files from the MWTM, why does TFTP fail or time out?, page C-14.

This section contains:

Setting Up TFTP on Solaris

To set up TFTP on your Solaris server:

Step 1 Verify that the tftp-server package is installed:

```
pkginfo -l | grep tftp
```

If the tftp-server package is not installed, install it from your Solaris CD or distribution.

Step 2 If you are not logged in, log in as the root user:

```
> login: root
> Password: root-password
```

If you are already logged in, but not as the root user, use the **su** command to change your login to root:

```
# su
# Password: root-password
```

Caution As the root user, 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 the root user to the tasks described in this manual.

Step 3 Using a UNIX editor, open the *inetd.conf* file:

```
/etc/inetd.conf
```

Step 4 In the *inetd.conf* file, ensure that this line appears:

```
tftp dgram udp6 wait root /usr/sbin/in.tftpd -s /tftpboot
```

If the line begins with a # sign, delete it, and save the changes.

Step 5 Ensure that this directory exists:

```
/tftpboot
```

If not, then create this directory. Also ensure the directory has write permissions (777).

Step 6 If you will be accessing more than one type of file (route, GTT, or MLR address table files,) you must create subdirectories, for example:

```
/tftpboot/route
/tftpboot/gtt
/tftpboot/atbl
```

Step 7 Restart the inetd process:

a. As the root user, enter:

```
# ps -ef | grep inetd
```

Output should be similar to:

```
root   157     1  0   Oct 21 ?        0:00 /usr/sbin/inetd -s
```

b. To find the process ID for inetd, enter:

```
# ps -e -o pid,comm | grep inetd
```

Output should be similar to:

```
157 /usr/sbin/inetd
```

c. To restart the inetd process, enter:

```
# kill -HUP 157
```

Where 157 corresponds to the output integer returned in Step b.

Step 8 Within the */opt/CSCOsgm/bin* directory, set the staging directory with these commands. For:

- Route table files, use the **mwtm routedir** command (see mwtm routedir, page B-114).
- GTT files, use the **mwtm gttdir** command (see mwtm gttdir, page B-98).
- MLR address table files, use the **mwtm atbldir** command (see mwtm atbldir, page B-90).

Setting Up TFTP on Linux

To set up TFTP on your Linux server:

Step 1 Verify that the tftp-server package is installed:

```
rpm -q tftp-server
```

If the tftp-server package is not installed, install it from your RedHat Enterprise CD or distribution.

Step 2 If you are not logged in, log in as the root user:

```
> login: root
> Password: root-password
```

If you are already logged in, but not as the root user, use the “su” command to change your login to root:

```
# su
# Password: root-password
```

Caution As the root user, 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 the root user to the tasks described in this manual.

Step 3 Using a UNIX editor, open the *tftp* file:

```
/etc/xinetd.d/tftp
```

Step 4 Edit the file:

a. Change the line:

```
user = nobody
```

to

```
user = root
```

b. Change the line:

```
disable = yes
```

to

```
disable = no
```

c. If you want to specify a different TFTP directory, replace */tftpboot* in the line *server_args = -s /tftpboot* with the name of your directory.

Step 5 Save the changes.

Step 6 Enter:

```
/etc/init.d/xinetd restart
```

Step 7 Set the staging directory:

- For route table files, use the mwtm routedir command (see mwtm routedir, page B-114).
- For GTT files, use the mwtm gttdir command (see mwtm gttdir, page B-98).
- For MLR address table files, use the mwtm atbldir command (see mwtm atbldir, page B-90).

Configuring Nodes

If MWTM User-Based Access is disabled, or if it is enabled and you are a Network Administrator or System Administrator, you can use the MWTM to view and change SNMP settings and configure login credentials.

For more information about user authorization levels in the MWTM, see Configuring MWTM User Account Levels (Server Only), page 2-7.

To access SNMP and credentials configuration, choose **Network > Node SNMP and Credentials Editor** from the MWTM main menu. The MWTM displays the Node SNMP and Credentials Editor dialog box.

The Node SNMP and Credentials Editor dialog box contains:

- Node SNMP and Credentials Menu, page 3-15

Node SNMP and Credentials Menu

The menu on the Node SNMP and Credentials Editor dialog box contains:

Menu Command	Description
File > Save (Ctrl-S)	Saves any SNMP configuration changes. When you are satisfied with all of your changes to the SNMP settings, choose the **File > Save** menu option. The MWTM saves the changes and updates the SNMP information on the MWTM server in real time. **Note** If another user modifies and saves the SNMP configuration before you save your changes, the MWTM asks if you want to overwrite that user's changes. If you choose to do so, the other user's changes are overwritten and lost. If you choose not to do so, your changes are lost.
File > Close (Ctrl-W)	Closes the current window. You may be prompted to save the current changes.
Help > Topics (F1)	Displays the table of contents for the MWTM online help.
Help > Window (Shift-F1)	Displays online help for the current window.
Help > About (F3)	Displays build date, version, SSL support, and copyright information about the MWTM application.

Configuring SNMP Settings

Note If you want to change SNMP settings, do so *before* running discovery.

For more information about SNMP, refer to "Configuring SNMP Support" in the Cisco IOS Release 12.2 *Configuration Fundamentals Configuration Guide*, Part 3, System Management.

To change SNMP settings in the MWTM, start the MWTM client, as described in Starting the MWTM Client, page 4-2, then choose:

- From the MWTM main window—**Network > Node SNMP and Credentials Editor** from the MWTM main menu.
- From the Discovery Dialog—**Edit > Node SNMP and Credentials Editor** from the menu bar.

Note (If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator [level 4] and higher.)

The MWTM displays the SNMP tab.

The SNMP tab of the Node SNMP and Credentials Editor dialog box contains:

- SNMP Settings Table, page 3-16
- SNMP Configuration Table, page 3-16
- SNMP Configuration Buttons, page 3-18

The MWTM also provides a set of commands that you can use to configure SNMP settings (see SNMP Configuration Commands, page 3-18).

SNMP Settings Table

The SNMP settings table displays current SNMP information for nodes in the MWTM. You can edit these fields in the SNMP Configuration Table, page 3-16.

The SNMP configuration table contains:

Column	Description
IP Address Range or Hostname	IP address or DNS name of a node or range of nodes. An asterisk (*) indicates a wildcard value.
Read Community	SNMP community name used by the node for read access to the information maintained by the SNMP agent on the node.
Timeout (secs)	Time, in seconds, the MWTM waits for a response from the node.
Retries	Number of times the MWTM attempts to connect to the node.
Poll Interval (mins)	Time, in minutes, between polls for the node.

SNMP Configuration Table

In the SNMP configuration table, you can change SNMP settings for a node.

The SNMP configuration table contains:

Field	Description
IP Address Range or Hostname	IP address or DNS name of a node. To change the IP address or DNS name of a node, select the node, enter the new address or name in the IP Address Range or Hostname field, then click **Update**. IP addresses use the format *x.x.x.x*, where each *x* has one of these values: • An integer in the range 0 through 255. • A range of integers separated by a hyphen (-), such as 10-60. • An asterisk (*), which is equivalent to specifying 0-255. The default value for this field is the IP address *.*.*.*, which the MWTM uses for all nodes not covered by other IP address ranges or names. When entering an IP address: • Use Class A, B, or C addressing: – Class A—The first octet value is within the range of 1-126. A valid IP address is from 1.0.0.1 to 126.255.255.254. – Class B—The first octet value is within the range of 128-191. A valid IP address is from 128.1.0.1 to 191.254.255.254. – Class C—The first octet value is within the range of 192-223. A valid IP address is from 192.0.1.1 to 223.255.254.254. • Do not use 0 or 255 for the last octet (*x.x.x.*0 is reserved for subnet addresses or network addresses; *x.x.x.*255 is reserved for subnet broadcast addresses). • Do not use IP addresses that fall within these ranges: 127.0.0.1-127.255.255.254, 128.0.0.1-128.0.255.254, 191.255.0.1-191.255.255.254, 223.255.255.1-223.255.255.254, and so on. • Do not use 0 for the first octet. Unlike IP addresses, you cannot specify a range of node names or use wildcards in node names. Each node name corresponds to a single node in the network.
Read Community	SNMP community name to be used by the node for read access to the information maintained by the SNMP agent on the node. To change the SNMP community name for a node, select the node and enter the new name in the Read Community field, then click **Update**. This new SNMP community name must match the name used by the node. The default name is *public*. For information about exporting SNMP community names from CiscoWorks Resource Manager Essentials (RME), see Importing SNMP Community Names from CiscoWorks (Solaris Only), page 3-2.

Field	Description
Timeout (secs)	Time, in seconds, the MWTM waits for a response from the node. If you determine that the MWTM waits too long for a response from a node, or does not wait long enough, you can change the timeout value. To change the time that the MWTM waits for a response from a node, select the node and enter the new timeout value in the Timeout (secs) field, then click **Update**. The valid range is 1 to 60 seconds. The default value is 1 second.
Retries	Number of times the MWTM attempts to connect to the node. If you determine that the MWTM retries a node too many times, or not enough times, you can change the number of retries. To change the number of times the MWTM attempts to connect to a node, select the node and enter the new number in the Retries field, then click **Update**. The valid range is 0 to 99. The default value is 2 retries.
Poll Interval (mins)	Time, in minutes, between polls for the node. If you determine that the MWTM polls a node too often, or not often enough, you can change the poll interval. To change the time, in minutes, between polls for a node, select the node and enter the new interval in the Poll Interval (mins) field, then click **Update**. The valid range is 5 to 1440. The default value is 15 minutes.

SNMP Configuration Buttons

The SNMP tab of the Node SNMP and Credentials Editor dialog box contains:

Button	Description
Add	Adds the new SNMP settings to the MWTM database. To add a new node or range of nodes, enter the SNMP information in the appropriate fields and click **Add**. The new SNMP settings are added to the MWTM database.
Update	Applies the values in the SNMP configuration fields to the selected node or range of nodes.
Delete	Deletes the selected node or range of nodes. To delete a node, select it and click **Delete**. The MWTM deletes the node without asking for confirmation.

SNMP Configuration Commands

This section contains:

MWTM Commands for SNMP

The MWTM provides these SNMP-related commands:

Command	Description
mwtm addsnmpcomm	Adds an SNMP configuration.
mwtm deletesnmpcomm	Deletes an SNMP configuration.
mwtm modifysnmpcomm	Modifies an existing SNMP configuration.
mwtm showsnmpcomm	Shows SNMP configuration(s).
mwtm snmpcomm	Sets a new default SNMP read community name.
mwtm snmpconf	Changes the file used for SNMP parameters, such as community names, timeouts, and retries.
mwtm snmpget	Queries a host using an SNMP GET request.
mwtm snmpnext	Queries a host using an SNMP GETNEXT request.
mwtm snmpsetup	Sets up SNMP configuration(s).
mwtm snmpwalk	Queries a host using an SNMP GETNEXT request or an SNMP GETBULK request to "walk" through the MIB.

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

Required SNMP Configuration for RAN-O Nodes

Configure these SNMP statements on the RAN-O nodes that you would like to manage by using the MWTM:

```
ipran-mib snmp-access <inBand | outOfBand>
ipran-mib location <cellSite | aggSite>
logging traps informational

snmp-server enable traps syslog
snmp-server community <SNMP_COMMUNITY_STRING> RO 1
snmp-server trap link ietf snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran snmp-server enable traps cpu threshold
snmp-server host <SNMP_SERVER_HOST_IP_ADDRESS> version 2c v2c
```

Tip For more information about these commands, refer to the *Cisco MWR 1941-DC-A Mobile Wireless Edge Router Software Configuration Guide.*

Configuring Login Credentials

This section contains:

You can use the MWTM to set up log in credentials, which you may use for:

Action	Description	Related Content
Troubleshooting	All networks	Viewing Troubleshooting
Discovery	ONS nodes only **Note** Only ONS nodes require login credentials during discovery; all other node types only require an SNMP community string.	Discovery Overview
Deployment	ITP only	Deploying ITP Files
Provisioning	All networks	Using Provisioning
Launching an SSH terminal to a node	All networks In the MWTM client navigation tree, right-click on an object and choose **Node > Connect to**.	Viewing the Right-Click Menu for an Object
Establishing a low-level connection to a node	ITP only In the MWTM client, choose **Network > Node File Management**, then choose **File > Connect** or In the Route Table Editor, choose **File > Deploy** or In the Global Title Translator Editor or Address Table Editor, choose **File > Load from Node** or **File > Deploy**.	Node File Management Deploying ITP Files Loading a GTT File from a Node Loading an Address Table File from a Node

Setting Up Login Credentials

The MWTM enables a system administrator to configure the login credentials using the Node SNMP and Credentials Editor dialog box. Login credentials are stored in an encrypted file on the server, eliminating the need for users to login before running commands.

To set up login credentials in the MWTM, start the MWTM client, as described in Starting the MWTM Client, page 4-2, then choose **Network > Node SNMP and Credentials Editor** from the MWTM main menu, and select the Credentials tab.

Note If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.

For detailed information on the SNMP tab, see Configuring SNMP Settings, page 3-15.

Tip A check mark appears beside nodes or default credentials that are configured.

A system administrator can set up credentials:

- Globally on all nodes of all types—Click **Default** and complete the fields in the right pane.
- All nodes of a specific node type only—Under Default, click the node type and complete the fields in the right pane.

Note Configuring default Cell Site Router (CSR) credentials applies to these CSRs: Cisco MWR and Cisco 3825.

- On a specific node—Under Nodes, click the node name and complete the fields in the right pane. Configuring credentials on a specific node overrides any Default credentials for that particular node.

The Credentials tab of the Node SNMP and Credentials dialog box contains:

- Credentials Fields, page 3-21
- Credentials Buttons, page 3-22

The MWTM also provides a set of commands that you can use to configure SNMP settings (for details, see the Credentials Commands, page 3-23).

Credentials Fields

Under the Credentials tab of the Node SNMP and Credentials dialog box, you can configure these login credentials for node(s):

Note Ensure that each user has sufficient privileges to run all commands.

Field	Description
IP Address or DNS Hostname	See Adding Nodes, page 3-23.
User name	Enter the login user name, if required.
Password	Enter the login password, if required.
Enable User name	Enter the login enable user name (not required for ONS nodes).

Field	Description
Enable Password	Enter the login enable password (not required for ONS nodes).
Connection Protocol	Choose the protocol to use when connecting to the node, either SSH or Telnet. **Note** The key size on the node must be configured to a minimum of 768 bits and a maximum of 2048 bits.

Note User name and password requirements vary according to your security configuration. For more information, see the *Cisco IOS Security Configuration Guide, Release 12.2*, Part 1 and Part 5.

Credentials Buttons

The Credentials tab of the Node SNMP and Credentials dialog box contains:

Button	Description
Apply	Applies specified user names and passwords to the selected node or Default credentials.
Clear	Removes credentials. To clear user names and passwords on a selected object, click **Clear** to remove the credentials, then click **Apply**.
Test	You can test the credentials you have configured on the corresponding node or the default credentials against a selected node type (not available for all node types).
Add	(Button only available when you click Nodes) Adds a specified node.

Adding Nodes

In the Credentials tab, you can add a node. If you are working with ONS nodes, you must add the ONS node and set the credentials for the node before running discovery.

Step 1 Click **Nodes** in the navigation tree.

Step 2 Enter the IP address or DNS host name.

Step 3 Add the user name and password credentials.

Step 4 Specify the connection protocol (Telnet or SSH).

Step 5 Click **Add**.

Credentials Commands

The MWTM also provides credentials-related commands:

- To add credentials for a given IP address, or for the Default credentials, use the mwtm addcreds command.
- To show credentials for a given IP address, or for the Default credentials, use the mwtm showcreds command.
- To delete credentials for a given IP address, or for the Default credentials, use the **mwtm deletecreds** command.

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

Creating New Troubleshooting Categories and Commands

A system administrator can use the MWTM to create user-specific categories and commands:

Step 1 On the server machine, if you are not logged in, log in as the root user:

```
> login: root
> Password: root-password
```

If you are already logged in, but not as the root user, use the "su" command to change your login to root:

```
# su
# Password: root-password
```

Caution As the root user, 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 the root user to the tasks described in this manual.

Step 2 Using a UNIX editor, open the *UserCommands.ts* file:

```
/opt/CSCOsgm/etc/UserCommands.ts
```

Step 3 Create new categories and commands, following the instructions in the *UserCommands.ts* file. Sample categories and commands are provided, which may be directly useful in your network.

Step 4 Save changes. The new categories and commands now appear in the Troubleshooting tabs.

Related Topics

- Viewing Troubleshooting, page 8-43
- mwtm tshootlog, page B-77