



Mobile Wireless Fault Mediator Release 2.2.1 - Patch A - E Software Release Notes

April 20, 2004



Note

You can find the most current Cisco documentation on Cisco.com. This set of electronic documents may contain updates and modifications made after the hard-copy documents were printed.

These release notes for Mobile Wireless Fault Mediator 2.2.1, which forms a part of CiscoWorks 2000 for Mobile Wireless bundle, describe the features provided in Release 1.2.

For a list of the software caveats that apply to MWFM, see the [“Caveats for Mobile Wireless Fault Mediator 2.2.1”](#) section on page 9.

Contents

These release notes include the following topics:

- [About the CW4MW Release 1.2, page 2](#)
- [Cisco Mobile Wireless Fault Mediator 2.2.1 Features, page 3](#)
- [Notes and Cautions, page 6](#)
- [Caveats for Mobile Wireless Fault Mediator 2.2.1, page 9](#)
- [Patch A, page 11](#)
- [Patch B, page 12](#)
- [Patch C, page 13](#)
- [Patch D, page 15](#)
- [Patch E, page 19](#)



Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

- [Related Documentation, page 23](#)
- [Obtaining Documentation, page 24](#)
- [Obtaining Technical Assistance, page 25](#)

About the CW4MW Release 1.2

CiscoWorks2000 for Mobile Wireless (CW4MW) is a suite of EMS applications that enhances the delivery of new mobile wireless services leveraging Cisco Mobility Platforms. It is comprised of:

- CiscoWorks 2000 LMS bundle, April Refresh
- CiscoWorks 2000 RWAN bundle, April Refresh
- Cisco APN Manager 2.0.1 (GPRS networks only), a carrier-class provisioning solution that automates the configuration process of APNs within a GPRS network to support a centralized GGSN access.
- Cisco Mobile Wireless Fault Mediator 2.2.1 (MWFM), a Telco-grade fault management solution that provides intelligent device discovery, and alarm filtering.
- CiscoView is a graphical SNMP based device management tool that provides real-time views of Cisco devices.

LAN Management

The LMS Bundle provides operationally focused applications for configuration, fault monitoring, and troubleshooting local networks. A browser interface provides easy-to-use access to topology maps, configuration services, and important system, device, and performance information. Because these applications are browser-accessible, administrators now have the freedom to access network tools anywhere from within the network.

Routed WAN Management

The Routed WAN Management Solution Bundle provides a collection of powerful applications to configure, administer, monitor, and troubleshoot routed wide-area networks, thereby dramatically reducing their complexity. This suite of solution applications provides increased visibility into network behavior and quickly identifies performance bottlenecks and long-term performance trends. It also provides sophisticated configuration tools to optimize bandwidth and utilization across expensive and critical WAN links in the network.

Access Point Name Management

For GPRS Networks only, the APN Manager provides flow-through management of APNs within the GPRS Support Node (GSN) complex to support centralized Public Data Network (PDN) access. It provides a **CORBA** interface to view and configure APN profiles in the GGSN and Domain Name Server (DNS) resource record from Network Management Systems (NMS) and other 3rd party Operations Support Systems (OSS).

Fault Mediation

Mobile Wireless Fault Mediator provides alarm filtering and correlation to the Gateway GPRS Support Node (GGSN) routers, Packet Data Serving Node routers in CDMA2000 networks, Mobile Wireless Routers (MWR1900) in an all IP-RAN network, and their neighboring Catalyst switches. In addition, it seamlessly integrates with Network and Service-layer Fault OSS to provide a complete network.

CiscoView

CiscoView for Cisco Devices is another Web based package for supporting the Wireless devices like GGSN, PDSN and MWR1900. This primarily provides a graphical representation of the device and indicates the state and status of the device's components such as ports, power supplies, etc.

CW4MW release 1.2.1 does not support a standalone version. The user has to install CW2000 solution CDs (either LMS bundle or RWAN bundle) along with CW4MW CDs including MWFM CD and APN manager CD.

For additional information on LMS & RWAN bundle refer to the following website:

<http://www.cisco.com/warp/public/44/jump/ciscoworks.shtml>

System Configuration Requirements

Table 1 lists the minimum system configuration needed for running CiscoWorks2000 Mobile Wireless Suite.

Table 1 Minimum System Configuration Requirements

Resource Component	CW2000 Suite for Mobile Wireless
Hardware	Sun Ultra 60 Workstation / SunFire 280R
Operating System	Solaris 7/8
Memory	4 GB RAM
Disk Space	18 GB Hard Disk
Processor	2 x 450Mhz
Swap space	2 X RAM
Operating Environment	CDE



Note

CD-One from either the LMS or the RWAN solution must be installed prior to MWFM or APN installation.

Cisco Mobile Wireless Fault Mediator 2.2.1 Features

MWFM is a feature-rich device layer solution that provides alarm filtering and correlation of Cisco Wireless Support Nodes (PDSN/GGSN) and their neighboring Catalyst Switches. This release also supports the Mobile Wireless Router (MWR1900) in an all IP-RAN Wireless network. MWFM uses

complex mathematics to solve the change monitoring problem allowing network management products such as Fault MoM to support networks that are experiencing the phenomenal growth imposed by the boom in Mobile Internet traffic.

Table 2 Cisco Mobile Wireless Fault Mediator 2.2 Features

Feature	Description	Benefit
Auto-Discovery	Automatically discovers Cisco GGSN/PDSN/MWR1900 network connections and changes while monitoring element status, including neighboring Catalyst switches	Provides a near real time model of the Cisco wireless network Eliminates manual update of network inventory
Complex Alarm Gathering Mechanism	SNMP Traps MIB Threshold Violation ICMP Polling	No additional configuration needed in the device Monitors key metrics in a preventive fashion and alerts NMS before condition negatively impacts the network performance Ensures devices are available
Multi NMS Support	Alarms can be forwarded to multiple NMS based on user-defined attributes	Allows a flexible integration with the SP NOC architecture
Filtering	Alarms can be filtered by alarm severity, device type, or alarm field	Empowers users to receive only the alarms that interest them and to hide the remaining ones from their view
Correlation	Alarm De-duplication of Alarms Reachability and device level correlation	Prevents users from being overflowed, particularly during an alarm storm. Provides the user with the probable root cause of alarms. This eliminates the guesswork of troubleshooting a network outage.
Standard Compliant	SNMP traps	Traps are forwarded to OSS based on SNMP standard
Integration with OSS and Fault MoM	Powerful query mechanism provide a synchronization facility with the OSS Standard Java API interface automates configuration and alarm synchronization between MWFM and OSS	In case of missed alarms or OSS crashing, users can retrieve a list of all active alarms via a Java API synchronization mechanism
AOC Browser	Configuration GUI that allow user to define rule sets	Removes the complexity of defining new correlation rules.
MWFM Faults Monitor Console	MWFM Alarm console allows the user to view all the active MWFM alarms and optionally delete any alarm.	Enables users to view active MWFM alarms in cases when integration with an SNMP Manager is not readily available.
Support for Sequential ID	All MWFM Alarms are tagged with a unique sequential ID.	Fault MoM can determine if it missed any MWFM alarms. Based on the IDs, it can request MWFM to resend alarms.

Table 2 Cisco Mobile Wireless Fault Mediator 2.2 Features (continued)

MWFM Administration Console	The user can configure MWFM using the MWFM Administration GUI	Configuration is further simplified over the CLI.
MWFM Device Monitor Console	User can view the devices being currently monitored as well as monitor faults /events for a particular device	A snap-shot of all of the devices in the network including the connectivity information available.
Enhanced Enable/Disable Feature	Operators can disable/enable traps for devices	Operator can ignore flood of alarms coming from certain devices
Device List export to RME	Operator can export MWFM device list to RME	Operator does not have to manually type in the IP addresses of the devices in RME
Support for Syslog Traps related to Flash	MWFM correlates Flash Syslog Traps sent by device	Operator is informed whenever the Flash card is removed/inserted from a device

Supported Hardware Platforms in MWFM 2.2.1

MWFM2.2.1 support the following devices:

- Catalyst 55XX family of switches
- Catalyst 6xxx family of L3 switches
- GGSN and PDSN routers (72xx, 75xx)
- HomeAgent (72xx)
- MWR1900 (19xx)

Supported Release Matrix for Platforms

Table 3 lists the supported releases.

Table 3 Supported Release Matrix

	Release	Routers
GGSN	1.4/3.0	72xx
PDSN	1.0/1.0.1	75xx
PDSN	1.0.2/1.1	72xx
HomeAgent	1.0/1.1	72xx
MWR1900	1.0	19xx

At the time of release, the following Cisco IOS images are supported by MWFM2.2.1:

- The Cisco IOS Images (PDSN 1.0)
rsp-g5isv-mz.121-3.XS
- The Cisco IOS Images (PDSN 1.0.1)
rsp-g5isv-mz.121-5.XS
rsp-g5isv-mz.121-5.XS1
rsp-g5is-mz.121-5.XS5
- The Cisco IOS Images (PDSN 1.0.2)
c7200-g5is-mz.r11.0718
- The Cisco IOS Images (PDSN 1.1)
c7200-g5is-mz.122-2.XC
c7200-g5is-mz.122-2.XC1
- The Cisco IOS Images (GGSN1.4)
c7200-g5js-mz.122-7.4
- The Cisco IOS Images (GGSN3.0)
c7200-g5js-mz.122-4.MX
- The Cisco IOS Images (HomeAgent 1.1)
c7200-is-mz.122-2.XC
c7200-is-mz.122-2.XC1
- The Cisco IOS Images (MWR1900 1.0)
mwr1900-i-mz.02182002
- The Cisco IOS image (MWR 1941-DC)
mwr1900-i-mz.122-8.MC2d

Notes and Cautions

MWFM 2.2.1

- MWFM Main Node renaming
For Root Cause analysis to report correctly the MWFM Server has to be renamed to fully qualified name (FQN). This shall be of the type <mwfm_server>.<domain_name>.com
- MWFM2.2.1 can listen only to SNMP version 1 traps.
All the devices should be configured to send traps in v1 format to MWFM2.1. Refer to the Cisco website for SNMPv1 configuration details.
<http://www.cisco.com/univercd/home/home.htm>
MWFM2.2.1 can send out only SNMPv1 traps to Northbound/Westbound NMS.
Northbound/West Bound NMS should be configured to listen to SNMPv1 traps

- Beta version of the AOC browser has been included with this release which configures most of the AOC file parameters. Additional parameters in the AOC files can be modified using any text editor (e.g., vi).



Note During installation if port 162 is in use then MWFM2.2.1 is configured to listen on port 45000 automatically. The application listening on port 162 has to be configured to forward the traps to MWFM2.1 on port 45000. Refer the appropriate documentation for configuring the application to forward traps to MWFM.

- If DFM is installed prior to MWFM
MWFM will be configured to use port 45000 automatically. The user will have to manually configure DFM to forward device traps to MWFM on port 45000.
- If RTM or HPOV is installed prior to installing MWFM and DFM
When MWFM is installed, it will be configured to use port 45000. The trapmux supplied with MWFM must be configured to listen to device traps on port 162 and forward these traps to MWFM and RTM or HPOV. The user must configure RTM or HPOV to listen for device traps from the MWFM trapmux.
- If MWFM is installed prior to RTM or HPOV and DFM is not installed
When MWFM is installed, it will be configured to use port 162. The trapmux supplied with MWFM must be configured to listen to device traps on port 162, and MWFM needs to be reconfigured to listen on port 45000. Forward these traps to MWFM and RTM or HPOV. Configure RTM or HPOV to listen for device traps from the MWFM trapmux.
- MWFM username and password for riv_oql.
The user name and password for executing riv_oql queries are 'admin', and '<BLANK>'
- Duplicate MAC Address
In the event an ARP table reports the same MAC address for multiple interfaces on the MWFM server, MWFM will not discover the devices properly.
To resolve this problem follow the steps listed below.

Step 1 Go to the Server boot prompt by pressing **Stop+A** keys at the same time

Step 2 Type the following command:

```
ok> setenv local-mac-address? true
```

Step 3 To restart the Sun machine, type the following command:

```
ok> reset
```

- MWFM does not forward event traps (uncorrelated traps) by default
User can turn on this capability by editing
\$RIV_HOME/etc/DistSchema.cfg.
The following steps show what needs to be done.

Step 1 Go to the line

```
insert into listeners.snoopers values (
  'TrapEvents1', 'Events', '<domain name>', 'Dist=1 AND EventName<>"EventTrap"',
  'TrapAdapt1', [{ } ]
);
```

Step 2 Change the above statement to

```
insert into listeners.snoopers values(
  'TrapEvents1', 'Events', '<domain name>', 'Dist=1', 'TrapAdapt1', [{ } ]
);
```

The above changes should be redone if a new NMS is added or modified using the configuration GUI.

- MWFM Trap varbinds - rivExtraInfo
rivExtraInfo field is truncated if it exceeds 256 characters.
- MWFM Server name needs to be registered in the DNS for the MainNode discovery and connectivity to other devices to work.
- On the MWFM GUI Administration Console, the user has to provide non-overlapping sequence IDs for trap receivers under "Add NMS" screen option.
- After installation/upgrading to MWFM 2.2.1, make sure that you clear the browser cache before pointing the browser at MWFM server.
- In order to use MWFM Disable/Enable feature at least one northbound NMS destination should be configured in MWFM. You can use the "Mobile Wireless Fault Mediator/Administration Console/Add NMS" window to add NMS destinations.

MWFM2.2.1 TCP/IP Port Assignments

The following TCP/IP ports are used by the applications in CW4MW1.2.1 suite.

MWFM 2.2.1 Trapmux	tcp/162
MWFM 2.2.1 Trap Monitor	tcp/45000
TIBCO/Rendezvous daemon	tcp/45001
MWFM 2.2.1 Trap Finder	tcp/45002
RTM	udp/395 (default udp/162)
DFM	udp/9000 (default udp/162)

Caveats for Mobile Wireless Fault Mediator 2.2.1

Caveats describe unexpected behavior in Cisco software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. Only select severity 3 caveats are included in the caveats document.

This section contains only open and resolved caveats for CiscoWorks2000 for Mobile Wireless Release 1.2.1.



Note

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, **log in** to Cisco.com and click **Software Center: Cisco IOS Software: Bug Toolkit: Bug Navigator II**. Another option is to go to <http://www.cisco.com/support/bugtools/>.

Open Caveats—Mobile Wireless Fault Mediator 2.2

This section documents possible unexpected behavior by CiscoWorks2000 for Mobile Wireless and describes only severity 1 and 2 caveats and select severity 3 caveats.

Bug ID and Description

- CSCdu84916

Symptom—AOC Browser - Fault Rule editor window comes up blank. Conditions: In the AOC Browser window click on the Methods icon under Fault the Fault Rule editor window comes up as a blank window

Workaround—Add the correlation rules by modifying the AOC files directly using a text editor.

- CSCdv63919

Symptom—MWFM riv2trap memory utilization too high.

Workaround—There are no known workarounds.

- CSCdx2982

Symptom—amos and riv_m_agents get restarted after rediscovery. Incoming events (new alarm/clear) might be lost after rediscovery.

Workaround—none

- CSCdu81757

Symptom—MWFM does not clear unknown traps after 24 hours.

Workaround—Unknown traps can be cleared either via Java API or by executing the following OQL :

```
lmwfm20:1> delete from mojo.events where EventType=0;lmwfm20:2> send;
```

- CSCdx40489

Symptom—CISCO-STP-EXTENSION-MIB related traps are not translated by MWFM.

Condition—When unprocessed traps are enabled.

Workaround—Perform the following steps to resolve this problem:

-
- Step 1** Download CISCO-STP-EXTENSION-MIB-V1SMI.my from:
ftp://ftp.cisco.com/pub/mibs/v1/CISCO-STP-EXTENSIONS-MIB-V1SMI.my
 - Step 2** Rename the MIB as CISCO-STP-EXTENSIONS-MIB-V1SMI.mib
 - Step 3** Copy the above MIB to /opt/CSCOPx/objects/mwfm/mibs/ directory.
 - Step 4** Stop MWFM (by issuing stop_mwfm).
 - Step 5** Delete all the files under /opt/CSCOPx/objects/mwfm/cache/
 - Step 6** Start MWFM (by issuing start_mwfm). The CISCO-STP-EXTENSION-MIB traps will be correctly translated by MWFM.
-

- CSCdx44231
Symptom—MWFM Trap might not be correctly decoded on some NMS.
Condition—rivLocation,rivContact,rivAssignedTo Varbinds missing from MWFM trap.
Workaround—Using text editor, modify RiverSoftTraps.mib (located in/opt/CSCOPx/objects/mwfm/mib directory) as follows:
-

- Step 1** Remove the text highlighted below

```
.rivEventTrap TRAP-TYPEENTERPRISE riversoftVARIABLES
{rivSequentialID,rivEntityName,rivCreateTime,rivDescription,rivCauseType,rivEventId,rivLocation,rivSeverity,rivExtraInfo,rivClassName,rivEventName,rivEventType,rivContact,rivAssignedTo,rivAcknowledged,rivCorrelatedId,rivEventGroupId,rivActionGlyph,rivOccurred,rivActionType,rivAgentAddresses,rivInternalAction
```
 - Step 2** Compile the above modified MIB with the NMS. This will enable the NMS to correctly decode MWFM traps.
-

- CSCdx81750
Symptom—MWFM does not cache Alarms.
Condition—When at the startup time, the user responds with "y" to the following prompt..."Do you want to delete the old MWFM Alarms (y/n):[n]"
Workaround—Do not respond with "y" to the above question. If you already responded with "y", then you can recover out of it by following the procedure described below.
-

- Step 1** Stop MWFM.
 - Step 2** Remove all the files from /opt/CSCOPx/objects/mwfm/cache/ directory
 - Step 3** Start MWFM
-

- CSCdy14669
Symptom—The MWFM 2.2.1 is not processing direct syslogs from devices. Not all devices support the Syslog traps For example, GGSN do not send syslog traps despite configuring the router with snmp-server enable traps syslog. Homeagent does not support Flash traps not Syslog traps.
Workaround—None
- CSCdy06894
Symptom—The import database takes in only one RO community string defined in MWFM IF there are multiple RO community strings defined in MWFM, they are not handled during import and therefore RME will fail to manage those devices.
Workaround—Manually modify the community Strings for the device via RME GUI interface.
Appendix A

Patch A

New Features/Fixes in MWFM2.2.1 Patch A:

- MWFM does perform DNS lookup for the discovered devices.
- Problem with null device display in Device Alerts/Events window is fixed.

Install Instructions

Step 1 Untar/Unzip the file (only if it is delivered as a tar/zip file)

```
# gunzip -c MWFM_2.2.1_Patch_A.tar.gz | tar -xvf -
```

Step 2 Change directory to "disk2"

```
# cd disk2
```

Step 3 Start the Patch Add program

```
# ./patchadd.sh
```

The MWFM 2.2.1 Patch A will be installed. Make sure that you start MWFM after installing the patch.

Uninstall Instructions

Step 1 Untar/Unzip the file (only if it is delivered as a tar/gzip file)

```
# gunzip -c MWFM_2.2.1_Patch_A.tar.gz | tar -xvf -
```

Step 2 Change directory to "disk2"

```
# cd disk2
```

Step 3 Start the Patch Remove program

```
# ./patchrm.sh
```

The MWFM 2.2.1 Patch A will be removed. Make sure that you start MWFM after un-installing the patch.

Patch B

New Features/Fixes in MWFM2.2.1 Patch B:

- Support for RMON traps (avgBusy5, bufferElFree, freeMem & generic RMON traps).
- Support for LNM Syslog Traps.
- Fix for bug id CSCea28789: MWFM cannot discover IP Addresses like A.B.C.0 or A.B.C.255

This patch also includes contents of MWFM 2.2.1 Patch A:

- MWFM performs DNS lookup for the discovered devices.
- Problem with null device in Device Alerts/Events window is fixed.

Install Instructions

Step 1 Untar/Unzip the file (only if it is delivered as a tar/gzip file)

```
# gunzip -c MWFM_2.2.1_Patch_B.tar.gz | tar -xvf -
```

Step 2 Change directory to "disk2"

```
# cd disk2
```

Step 3 Start the Patch Add program

```
# ./patchadd.sh
```

The MWFM 2.2.1 Patch B will be installed. Make sure that you start MWFM after installing the patch.

Un-install Instructions

Step 1 Untar/Unzip the file (only if it is delivered as a tar/zip file)

```
# gunzip -c MWFM_2.2.1_Patch_B.tar.gz | tar -xvf -
```

Step 2 Change directory to "disk2"

```
# cd disk2
```

Step 3 Start the Patch Remove program

```
# ./patchrm.sh
```

The MWFM 2.2.1 Patch B will be removed. Make sure that you start MWFM after un-installing the patch.

Patch C

New Features/Fixes in MWFM2.2.1 Patch C:

- CSCea77726—Critical ping fail alarms on Loopback 2 forwarded from MWFM.
- CSCea77767—MWFM does not allow to enter network 10.255.0.0 into discovery scope.
- CSCea77743 —No explicit alarm for MWR1900 fail over.

The following has been done to resolve CSCea77743:

- State change of the Loopback102 is detected and based on whether the interface goes from down to up OR up to down, the FailoverDetectedActive & FailoverDetectedActive alarm is generated.
- HSRP state (Active/Standby) of the device is maintained based on the following sources:
 - cHsrpStateChange trap from the device.
 - Mini-RMON process configured to monitor cHsrpGrpStandbyState (See the section [HSRP Monitoring, page 15](#))



Note Additional configuration is required on the device.

- Status of Loopback102 interface which is retrieved via SNMP Poll every 3 hours.
- It is recommended that the following configuration be added to the MWR1900 so that they can retain the ifIndex for the interfaces ever after reboot.
 - "snmp-server ifindex persist"



Note The Interface table is now polled every 3 hours instead of current 10 minutes.

This Patch also includes contents of MWFM2.2.1 Patch B:

- Support for RMON traps (avgBusy5, bufferElFree, freeMem & generic RMON traps).
- Support for LNM Syslog Traps.
- Fix for Bug id: CSCea28789 - MWFM cannot discover IP Addresses like A.B.C.0 or A.B.C.255.

This Patch also includes contents of MWFM2.2.1 Patch A:

- MWFM performs DNS lookup for the discovered devices.
- Problem with null device in Device Alerts/Events window is fixed.

Latest Patches

For information on the latest MWFM patches, direct your browser to:

<http://www.cisco.com/cgi-bin/tablebuild.pl/fault-med>

Install Instructions

Step 1 Untar/Unzip the file (only if it is delivered as a tar/gzip file).

```
# gunzip -c MWFM_2.2.1_Patch_C_mmddyy.tar.gz | tar -xvf -
```

Step 2 Change directory to "disk2".

```
# cd disk2
```

Step 3 Start the Patch Add program.

```
# ./patchadd.sh
```

The MWFM 2.2.1 Patch C will be installed. Make sure that you start MWFM after installing the patch.

Uninstall Instructions

Step 1 Untar/Unzip the file (only if it is delivered as a tar/gzip file).

```
# gunzip -c MWFM_2.2.1_Patch_C_mmddyy.tar.gz | tar -xvf -
```

Step 2 Change directory to "disk2".

```
# cd disk2
```

Step 3 Start the Patch Remove program.

```
# ./patchrm.sh
```

The MWFM 2.2.1 Patch C will be removed. Make sure that you start MWFM after un-installing the patch.

HSRP Monitoring

Sample mini-rmon commands for HSRP monitoring are listed below.

```
rmon event 3 log trap public description "Router now active" owner cisco
rmon event 4 log trap public description "Router now standby" owner cisco
rmon alarm 2 cHsrpGrpEntry.15.1.1 180 absolute rising-threshold 6 3
falling-threshold 5 4 owner cisco
rmon alarm 3 cHsrpGrpEntry.15.2.2 180 absolute rising-threshold 6 3
falling-threshold 5 4 owner cisco
```

Patch D

New Features in MWFM2.2.1 Patch D:

- Support for MWR1941-DC.
- Ping poll frequency has been increased from 60 seconds to 900 seconds (*See Notes & Cautions, page 17* for recommendation pertaining to this change).
- Launching of MWFM Syslog Monitoring agent has been disabled by default.
- MWFM Log rotation tool which monitors the MWFM log file size has been added. The Logs are gzipped & rotated if they exceed 10 MB in size.
- Additional rules added to process & suppress FAN-4-FAN_FAILED & CONTROLLER-3-FIRMWARE Syslog Traps. MWFM de-duplicates the above alarms and reports the 1000th occurrence of the above alarm i.e. the 1st, 1001th, 2001th, etc., occurrence of the above alarm is reported to the northbound NMS (*See Notes & Cautions, page 17* for recommendation pertaining to the Syslog Traps).
- In order to clean unnecessary Events/Alerts and thus improve MWFM performance, the following Events/Alerts are automatically removed from MWFM System based on their age.
 - a. Unprocessed traps from Discovered Devices which are older than 60 seconds (This rule is fired every 5 minutes).
 - b. Unprocessed traps from undiscovered devices which are older than 60 seconds (This rule is fired every 5 minutes).
 - c. Any alarms with Severity =< MINOR which are older than 24 hours (This rule is fired every 3 hours).
 - d. Any alarms with Severity = MAJOR which are older than 3 days (This rule is fired every 12 hours).
 - e. Any alarms with Severity = CRITICAL which are older than 7 days (This rule is fired every 24 hours).
 - f. All non-LNM Syslog Traps which are older than 60 seconds (This rule is fired every 5 minutes).
- All the above Deleted Events/Alerts (Except bullets b & f) are written to deleted_alarms.txt file in the logs directory. Although bullets b & f are not written to a file by default, the administrator can enable writing of the above alarms to a file by following the procedure below.

Follow the instructions below to enable the logging.

Step 1 Stop MWFM

Step 2 Open /opt/CSCOpX/objects/mwfm/aoc/Core.aoc file in a text editor.

Step 3 Look for the following block on text

```
{
rulename = 'UnknownTrapDeleteFromUnknown',

... snipped for clarity ...

        change_events = [
//          {
//              action = {
//                  actionvalues = [
//                      "Description = eval(text, 'CAT('Timed Delete:
\,&&Description)') "
//                  ],
//                  filter="EventId=eval(int, '&&EventId') "
//              },
//              actionfilter="EventId=eval(int, '&&EventId') "
//          }

... snipped for clarity ...

        ],
}

```

Step 4 Remove the comment string "//". For example...

```
{
    action = {
        actionvalues = [
            "Description = eval(text, 'CAT('Timed Delete:
\,&&Description)') "
        ],
        filter="EventId=eval(int, '&&EventId') "
    },
    actionfilter="EventId=eval(int, '&&EventId') "
}

```

Step 5 Remove the following *Classes* files from the cache directory

```
# cd /opt/CSCOpX/objects/mwfm/cache
# rm *Classes*
```

Step 6 Start MWFM.

Closed Caveats in MWFM2.2.1 Patch D

- CSCeb80361—Incase of large network discovery, start_mwfm does not show the list of devices. The following error message is displayed ... "#Request Timed Out No service provider listening."
- CSCec03407—Configure_mwfm tool does not allow operator to enter 0 or 255 into one of the octets of the DNS Server IP. (MR int030151).
- CSCeb14228—Severity of LinkNoiseInterfaceRestored should be set to CLEAR(MR int030164).
- CSCec03426—The trap monitor agents gets stuck if it keeps on receiving traps while it is downloading the topology.
- CSCec03435—MWFM GUI times out when large number of Events/Alerts get accumulated in the MWFM database(MR int030099).

Notes & Cautions

- It is recommended that the generations of Syslog Traps should be disabled by default on the devices. However, for LinkNoiseMonitor(LNM) support, Syslog Trap should be enabled with severity level of LNM Syslog Trap & higher. For example, if the LNM Syslog severity is 4, then the operator should enable Syslog traps for severity 4,3,2,1 & 0. Similarly, if the LNM Syslog Severity is 1, then the operator should enable Syslog traps for severity 1 & 0. The operator can use the "logging history <severity_level>" IOS command to control the generation of Syslog Trap based on severity.
- Keeping large network in mind, currently the ping poll frequency has been set to 900 seconds so as to reduce the network management traffic. As a side affect, the operator will be observe ping failure alarms after 1 hour (MWFM reports ping failure alarms after 4 successive ping failure occurrences). It is recommended, that this poll frequency be reduced to lower number (for example, 60 seconds) incase of smaller networks.

Follow the instructions below to change the Ping Poll Frequency.

-
- Step 1** Stop MWFM
- Step 2** Open /opt/CSCOPx/objects/mwfm/aoc/Device.aoc file in a text editor.
- Step 3** Look for the following block on text

```

        { // Ping poll
          PollDefState=0,
... snipped for clarity ...

          Severity=3,
          Description="eval(text,'CAT(`Ping fail on device
`,this->EntityName)')",
          Location="",
          Contact="",
          EventName="pingFail",
          Frequency=900,
          Threshold= "",
          ThreshFailList={},

... snipped for clarity ...

        },

```

Step 4 Change the interval at which you want the Ping Poll to happen. For example:

```
Frequency=60,
```

Step 5 Remove the following *Classes* files from the cache directory

```
# cd /opt/CSCOpX/objects/mwfm/cache
# rm *Classes*
```

Step 6 Start MWFM

- With the new cleaning rules that are implemented in MWFM2.2.1 Patch D, the operator might see the following behavior:
 - Lets say some minor Alarm comes in from a device and the same is reported to northbound NMS.
 - Lets say even after 24 hours, MWFM has not received a clear alarm from the device. Based on the new MWFM cleaning rules, the above minor alarm will be removed from the system and the same will be notified to the northbound NMS.
 - However, lets say after 24 hours, the device reports the clear of the above alarm. In such case MWFM will not report the clear alarm to the northbound NMS.
-

Install Instructions

Step 1 Untar/Unzip the file (only if it is delivered as a tar/gzip file)

```
# gunzip -c MWFM_2.2.1_Patch_D_mmddyy.tar.gz | tar -xvf -
```

Step 2 Change directory to "disk2"

```
# cd disk2
```

Step 3 Start the Patch Add program

```
# ./patchadd.sh
```

The MWFM 2.2.1 Patch D will be installed. Make sure that you start MWFM after installing the patch.

Uninstall Instructions

-
- Step 1** Untar/Unzip the file (only if it is delivered as a tar/zip file)
- ```
gunzip -c MWFM_2.2.1_Patch_D_mmddy.tar.gz | tar -xvf -
```
- Step 2** Change directory to "disk2"
- ```
# cd disk2
```
- Step 3** Start the Patch Remove program
- ```
./patchrm.sh
```

The MWFM 2.2.1 Patch D will be removed. Make sure that you start MWFM after un-installing the patch.

---

## Patch E

New Features/Fixes in MWFM2.2.1 Patch E:

- MR # MOTCM00113463—Cisco TAC # E643098 new riv\_ctrl binary, The new riv\_ctrl binary will prevent ctrl from spawning multiple processes on missed heartbeats from all the MWFM processes
- MR # MOTCM00113463—riv\_check script change to remove egrep for Monitor and Dist processes and replace with 'ps-ef |grep'
- MR # MOTCM00118819—add CISCO-ACCESS-ENVMON-MIB trap support to the Cisco.aoc for caemTemperatureNotification caemVoltageNotification

## Incremental Discovery

MWFM supports two ways of discovering devices in a Network.

- Full Discovery
- Incremental discovery

MWFM Full discovery is intended for discovering the devices in a Network for the very first time when MWFM is installed. However, there are situations wherein some devices do not get discovered during Full Discovery cycle for various reasons. For example:

- Device being unreachable during full discovery.
- Device being heavily loaded due to which it is not able to respond to MWFM queries.
- Incorrect configuration on the device.
- New devices have been freshly deployed.
- MWFM Discovery uses the inband data channel to gather device information. Hence, during high traffic times, it is quite possible that a device may not get discovered if the discovery packets get dropped.

To discover and monitor such kind of devices, MWFM Incremental Discovery can be used.

## How to use Incremental Discovery

Primarily three steps are involved in discovering device via MWFM Incremental Discovery.

- Identifying the devices that need to be discovered using Incremental Discovery.
- Launching Incremental Discovery.
- Monitoring progress of Incremental Discovery.

---

### Step 1 Identifying the devices that need to be discovered using Incremental Discovery.

There are two ways to identify these devices by doing the following:

- a. If the list of devices that need to be incrementally discovered are already known, then the user can directly populate "list\_of\_devices.txt" file.

Open the /opt/CSCOpX/objects/mwfm/scripts/list\_of\_devices.txt using any text editor.




---

**Note** The "list\_of\_devices.txt" file may have to be created if it does not exist.

---

- b. Add the devices that hat need to be submitted to MWFM Incremental Discovery

12.12.12.4

12.12.12.7

- c. If the list of devices that need to be incrementally discovered is not known, then the user generate the list by following the procedure below.

Open the /opt/CSCOpX/objects/mwfm/scripts/master\_device\_list.txt file in some text editor.

- d. Add all the list of devices that exist in the network as follows:

12.12.12.1

12.12.12.2

12.12.12.3

12.12.12.4

12.12.12.5

12.12.12.6

12.12.12.7

12.12.12.8

12.12.12.9

- e. Execute find\_undiscovered\_devices.sh

```
cd /opt/CSCOpX/objects/mwfm
ksh
. ./mwfm.kshrc
cd scripts
cd /opt/CSCOpX/objects/mwfm/scripts
./find_undiscovered_devices.sh
```

This script will compare the devices in master\_device\_list.txt with the one MWFM is currently monitoring. The devices which are not currently discovered/monitored by MWFM will be written to "list\_of\_devices.txt"

**Step 2** Launching Incremental Discovery.

The devices that need to be incrementally discovered have been identified, the user can invoke incremental discovery as follows:

```
pwd
/opt/CSCOpX/objects/mwfm/scripts
./incremental_disco.sh
```

The devices in the list\_of\_device.txt will be submitted to MWFM Incremental Discovery for further processing.

**Step 3** Monitoring progress of Incremental Discovery.

Issue the following commands to determine if MWFM Incremental discovery has finished or not.

```
cd /opt/CSCOpX/objects/mwfm/logs.WIRELESS
grep Completed ctrl.log
Phase 0 Completed Fri Apr 9 06:40:59 2004
Phase 1 Completed Fri Apr 9 06:42:33 2004
Phase 2 Completed Fri Apr 9 06:42:33 2004
Last Phase Completed Fri Apr 9 06:42:38 2004
Phase -1 Completed Fri Apr 9 06:44:45 2004
```

If following string "Phase -1 Completed" is observed towards the end, then that implies that incremental discovery has finished.



**Note** That multiple runs of incremental discovery might be needed for following reasons:

MWFM Discovery uses the inband data channel to gather device information. Hence, during high traffic times, it is quite possible that a device may not get discovered if the discovery packets get dropped.

That SNMP being UDP based is sometimes unreliable. MWFM Discovery relies on SNMP to gather Device information. Hence due to the unreliable nature of SNMP/UDP, MWFM may not be able to successfully gather device information and hence may drop the device in the middle of the discovery cycle.

It is quite possible that the device that MWFM is trying to discover is down or there is some kind of mis-configuration due to which MWFM is not able to discover the device. In such situations, it is recommended that configuration of the device be checked. Please also ensure that the device is pingable and that device does respond to SNMP queries.

## Install Instructions

**Step 1** Untar/Unzip the file (only if it is delivered as a tar/gzip file)

```
gunzip -c MWFM_2.2.1_Patch_E_mmddyy.tar.gz | tar -xvf -
```

**Step 2** Change directory to "disk2".

```
cd disk2
```

**Step 3** Start the Patch Add program

```
./patchadd.sh
```

The MWFM 2.2.1 Patch E will be installed.



**Note** Make sure you start MWFM after installing the patch.



**Note** It is recommended to save the disk2 directory on the machine. The save directory under the disk2 will be used during the patch removal process.

## Uninstall Instructions

**Step 1** Untar/Unzip the file (only if it is delivered as a tar/gzip file)  

```
gunzip -c MWFM_2.2.1_Patch_E_mmddy.tar.gz | tar -xvf -
```

**Step 2** Change directory to "disk2".  

```
cd disk2
```

**Step 3** Start the Patch Remove program  

```
./patchrm.sh
```

  
 The MWFM 2.2.1 Patch E will be removed.



**Note** Make sure you start MWFM after uninstalling the patch.

## Closed Caveats in MWFM2.2.1 Patch E

- CSCeb80361—Incase of large network discovery, start\_mwfm does not show the list of devices. The following error message is displayed. `.#Request Timed Out. No service provider listening.`
- CSCec03407—configure\_mwfm tool does not allow operator to enter 0 or 255 into one of the octets of the DNS Server IP. (MR int030151)
- CSCeb14228—Severity of LinkNoiseInterfaceRestored should be set to CLEAR(MR int030164)
- CSCec03426—The trap monitor agents gets stuck if it keeps on receiving traps while it is downloading the topology.
- CSCec03435—MWFM GUI times out when large number of Events/Alerts get accumulated in the MWFM database(MRint030099).
- CSCec03444—T1 Alarms are not getting processed.

## Related Documentation

The CiscoWorks2000 for Mobile Wireless documentation set is available online at:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2k4mw/index.htm>

- *Read Me First—Mobile Wireless Fault Mediator, Release 2.2*
- *Mobile Wireless Fault Mediator 2.2.1 Release Notes* (this document)
- *Cisco Mobile Wireless Fault Mediator Release 2.2; Fault Engine Reference Guide*
- *Cisco Mobile Wireless Fault Mediator Release 2.2; Topology and Platform Modeling Reference Guide*
- *Cisco Mobile Wireless Fault Mediator Release 2.2; Java API Guide*
- *Cisco Mobile Wireless Fault Mediator 2.2.1 - GUI User Guide*

# Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

## World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems  
Attn: Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

### Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

### Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

---

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratum, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)

Copyright © 2004, Cisco Systems, Inc. All rights reserved