Release Notes for MSS Version 7.1.7.2

Trapeze Networks, Inc.
5753 W. Las Positas Blvd.
Pleasanton, CA 94588
Tel: +1 925-474-2200
Fax: +1 925-251-0642
Toll-Free: 877-FLY-TRPZ (877-359-8779)

For the most current version of all documentation, go to
www.trapezenetworks.com

Part Number: 735-9502-0078 Rev H

Trapeze Networks recommends that you familiarize yourself with the Known Behaviors and Issues section in this document before installing Mobility System Software (MSS) Version 7.1. For additional product information, refer to the following manuals in addition to these release notes:

- *Mobility System Software Quick Start Guide*
- *Mobility Exchange Installation Guide*
- *Mobility Point Indoor MP Installation Guide*
- *Mobility Point MP-620 Installation Guide*
- *Regulatory Information*
- *Mobility System Software User's Guide*
- *Mobility System Software Command Reference*
- *RingMaster Planning Guide*
- *RingMaster Configuration Guide*
- *RingMaster Management Guide*

Feedback and Support

- Trapeze Networks encourages you to provide feedback about your experiences installing and using the product to the Trapeze Networks Technical Assistance Center (TAC). You can contact the TAC by telephone, e-mail, or fax. If you have a service contract or are a Trapeze Authorized Partner, log in to Trapeze SafetyNet Online at www.trapezenetworks.com/support/contact_support for additional help.
- Within the US and Canada, call 1-866-TRPZTAC (1-866-877-9822).
- From locations outside the US and Canada, call +1 925-474-2400.

- In non-emergencies, send email to support@trapezenetworks.com.

What's New in MSS Version 7.1

MSS Version 7.1 contains the following enhancements:

- **Trapeze Virtual Controller Cluster Enhancements** — MSS 7.1 continues to enhance the revolutionary Virtual Controller Cluster feature set. This release adds the following new functionality:
  - **AP Affinity** - AP Affinity allows a network operator to configure a preference for which controller APs connect to in non-failure scenarios. Groups are configured on each cluster member and are shared within the Cluster.
  - **Hitless software upgrade** - Network Resiliency enhancements in MSS 7.1 now allow you to optionally perform an in-service software upgrade. A coordinated upgrade of all controllers and APs in the cluster results in minimal service interruption for client devices.
  - **Licensing Changes** - The Virtual Controller Cluster feature is now part of the Trapeze High Availability Add-on Module. When using the HA license with the Virtual Controller Cluster features, redundant AP licenses are automatically created on Cluster members (1:1 for licensed APs, up to the controller platform max).
- **SIP Awareness** — Integrated stateful application awareness for the SIP protocol adds a new level of intelligence that allows granular and dynamic control of voice applications. Awareness of SIP call state allows for advanced QoS treatment, call-based Call Admission Control and Call Detail Record generation. The SIP Awareness feature set is enabled via the Advanced Voice Module software add-on.
- **LDAP Authentication Support** — MSS 7.1 introduces native LDAP as an available method for user authentication. This allows for an operator to deploy wireless services without requiring a RADIUS backend. LDAP authentication is supported for Web-Portal, MAC, and Administrative authentications.
- **Licensing Changes** — Starting in MSS 7.1 the current licensing model (AP licensing, FIPS licensing, etc) has been extended to support three new Feature License options. The following licenses are now available:
  - High Availability Module — covers the Virtual Controller Cluster feature set.
  - Advanced Voice Module — covers the SIP Awareness feature set including Dynamic CAC and Call Detail Records.
  - Mesh and Bridging Module — covers APs in Mesh and Bridge applications

Minor Enhancements

- **Security Features**
  - IPSec Client for secure RADIUS connections
  - Logging of RingMaster changes using Command Audit
  - Countermeasure support for Ad-hoc devices
  - Wired-auth session aging
  - Configurable RingMaster management port
  - Support for extended intermediate Certificate Authorities in Certificate path
  - SCP support for secure file copy operations

- **Supportability Features**
  - Scheduled command execution
  - Embedded TFTP server support
  - Improvements to 'show ap' output
- **AAA Features**
  - Support for Web-portal clients in local switching mode
  - Per-User authentication of RingMaster changes
  - 'service-type' based access to privileged CLI mode
  - Configuration control for Acct-interim-update per SSID
- **Mesh and Bridging Enhancements**
  - Mesh and Bridge services now support the use of "hidden" SSIDs for backhaul networks.
- **System Features**
  - Configurable support for AP "lights out" mode
  - 512 AP support for MX-2800

Version Compatibility

RingMaster

This version of Mobility System Software (MSS) is intended for use with RingMaster Version 7.1 or higher only.

Minimum MSS Requirements for Upgrade

Table 1– 1 lists the minimum MSS version an MX must be running when you upgrade to MSS Version 7.1. If your MX is running an older MSS version, you can use the upgrade path to upgrade the MX to 7.1.

Table 1– 1. Software Requirements for Upgrade to MSS Version 7.1

Product	Minimum MSS Version Required	Upgrade Path
MX-216 MX-200	5.*x*	5.0.15.2 -> 6.0.7.2 ->*7.0.x.x*->*7.1.x.x*
MXR-2	5.*x*	5.0.15.2 -> 6.0.7.2 ->*7.0.x.x*->*7.1.x.x*
MX-8	5.*x*	5.0.15.2> 6.0.7.2 ->*7.0.x.x*->*7.1.x.x*
MX-400	5.x	5.0.15.2 -> 6.0.7.2 ->*7.0.x.x*->*7.1.x.x*
MX-2800	7.0.3.6	7.0.x.x->*7.1.x.x*

With the release of MSS Version 7.0, the following MPs are no longer supported: MP-241, MP-252, MP-262, MP-341, and the MP-352.

Upgrading to MSS Version 7.1

Before you upgrade, see **"Version Compatibility" on page 4**. After you verify that the MX is running the minimum MSS version required to upgrade to MSS Version 7.1, return to this section.

VLAN IDs higher than 3520

To avoid conflicts with the Trapeze internal VLAN numbering scheme, it is strongly advised to use VLAN IDs less then 3520 on MXs that are upgrading to MSS Version 7.0. Failure to do so may result in lost configuration data.

Changes to file storage location

MSS 7.1. includes changes to the storage location of system debug files. Debug information is now stored in persistent user-accessible storage for retrieval after a system restart.

Preparing the MX for the Upgrade

Create a backup of your MX files before you upgrade the MX.

Trapeze Networks recommends that you make a backup of the MX, before you install the upgrade. If an error occurs during the upgrade, you can restore your MX to a previous configuration.

MSS 7.1 includes support for individual cipher configuration on both the WPA and RSN IEs. When downgrading from MSS 7.1 to an earlier version of MSS, changes to IE configuration will be lost.

You can use the following command to back up the configuration files:

backup system [**tftp:**/*ip-addr*/]*filename* [**all** | **critical**]

To restore an MX that is backed up, use the following command:

restore system [**tftp:**/*ip-addr*/]*filename* [**all** | **critical**]

"Upgrade Scenario" on page 6 shows an example of the **backup** command. For more information about these commands, see the "Backing Up and Restoring the System" section in the "Managing System Files" chapter of the *Trapeze Mobility System Software User's Guide*.

Upgrading an Individual MX Using the CLI

If you have made configuration changes but have not saved the changes, use the **save config** command to save the changes, before you backup the MX.

1. Back up the MX, using the **backup system** command.
2. Copy the new system image onto a TFTP server.

   For example, log into http://www.trapezenetworks.com/support/support_portal_login using a Web browser on your TFTP server and download the image onto the server.
3. Copy the new system image file from the TFTP server into a boot partition in the nonvolatile storage of the MX. For example,

   ```
   MX-200# copy tftp://10.1.1.107/MX071001.200 boot1:MX071001.200
   ```

   You can copy the image file only into the boot partition that was *not* used for the most recent restart. For example, if the currently running image was booted from partition 0, you can copy the new image only into partition 1.
4. Set the boot partition to the one with the upgrade image for the next restart.

   To verify that the new image file is installed, type **show boot**.
5. Reboot the software.

   To restart an MX and reboot the software, type the following command:

   reset system

When you restart the MX, the MX boots using the new MSS image. The MX also sends the MP version of the new boot image to MPs and restarts the MPs. After an MP restarts, the version of the new MP boot image is checked to make sure the version is newer than the version currently installed on the MP. If the version is newer, the MP completes installation of the new boot image by copying the boot image into the MP flash memory, which takes about 30 seconds, then restarts again. The upgrade of the MP is complete after the second restart.

Upgrade Scenario

To upgrade an MX-200, use the following upgrade example.

This example copies the image file into boot partition 1. On your MX, copy the image file into the boot partition that *was not* used the last time the MX was restarted. For example, if the MX booted from boot partition 1, copy the new image into boot partition 0. To see boot partition information, type the **show boot** command.

```
MX-200# save config
success: configuration saved.
MX-200# backup system tftp:/10.1.1.107/sysa_bak
success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
MX-200# copy tftp://10.1.1.107/MX071001.200 boot1:MX071001.200
.....................................................................
.....................................................................
.....................................success: received 10266629 bytes in 92.427
seconds [ 111078 bytes/sec]
MX-200# set boot partition boot1
```

```
success: Boot partition set to boot1:mx071001.200 (7.1.0.1).
MX-200# show boot
Configured boot version:         7.1.0.1
Configured boot image:           boot1:mx070001.200
Configured boot configuration:   file:configuration
Backup boot configuration:       file:backup.cfg
Booted version:                  7.1.0.1
Booted image:                    boot1:mx0701202.200
Booted configuration:            file:configuration
Product model:                   MX
MX-200# reset system
...... rebooting ......
```

Installing Upgrade Activation Keys on an MX

MSS 7.1 includes support for MP upgrade licenses and 3 new feature license options:

- Advanced Voice Module
- High Availability Module
- Mesh/Bridging Module

These feature license keys are installed alongside MP upgrade licenses. Additional details of the features/functionality included with each license are available in the product data sheets.

When installing MP based features licenses (e.g. Mesh/Bridging Module) the licenses should be installed on the MX where the MP is configured. For Cluster environments, licenses should be installed on the Cluster seed.

MP licensing is supported on MX platforms as shown in **Table 1– 2**:

Table 1– 2. Licensing and Upgrade Increments for the MX Models

MX Model	Base MP Support	Maximum MP Support	Upgrade Increment
MX-400	40	120	40
MX-200/ MX-216	32	192	32
MX-2800	64	512	64

If you downgrade to a previous version of MSS that does not support the higher capacity licenses, the number of allowed MPs is reduced to comply with the older software limitations and feature licenses are removed.

Feature licensing is supported on MX platforms as show in **Table 1– 3**.

Table 1– 3. MX Feature Licensing Matrix

MX Model	Advance Voice Module	High Availability Module	Mesh/Bridging Module
MXR-2	Supported	Not Supported	Up to 4 MPs (16 MPs in Cluster mode)
MX-8	Supported	Not Supported	Up to 12 MPs (48 in Cluster mode)
MX-400	Not Supported	Not Supported	Up to 120 MPs (480 MPs in Cluster mode)
MX-200 and MX-216	Supported	Supported	Up to 192 MPs (768 in Cluster mode)
MX-2800	Supported	Supported	Up to 512 MPs (4096 in Cluster mode)

To upgrade an MX license:

1. Obtain a license coupon for the upgrade from Trapeze Networks or your reseller.
2. Establish a management session with the MX to display the serial number. To display the serial number, type the following command:

   show license

   In the following example, the MX serial number is 123456789:

```
MX> show license

Serial Number        123456789

Platform AP Count    :   32 access points are supported
Licensed AP Count    :   96 aadditional access points

128 access points are supported

Additional Features:
                     Feature Description          Installed
-------------------------------------------------------------
```

3. Use a Web browser to access the Trapeze Networks license server at the following URL:

   http://www.trapezenetworks.com/support/product_licenses

4. Type your e-mail address in the E-mail and Confirm E-mail fields.
5. Select your MX model and feature license (if applicable) from the Product Selection list.
6. Type or copy and paste the MX serial number into the Product Serial Number field, and click **OK**. The Product Licensing page appears.
7. Type the coupon activation code(s) into the Coupon Code(s) fields and click **OK**. The Licensing Confirmation page appears, and displays the activation key (also called the license key).
8. Highlight and copy the entire activation key.
9. On the MX, use the following command at the enable (configuration) level of the CLI to install the activation key:

   set license activation-key

In the following example, an activation key for an additional 96 MPs is installed on an MX-200:

```
MX-200# set license 3B02-D821-6C19-CE8B-F20E
success: license accepted
```

10. Verify installation of the new license by typing the following command:

```
MX-200# show licenses
Serial Number        123456789

Platform AP Count    :   32 access points are supported
Licensed AP Count    :   96 aadditional access points

128 access points are supported

Additional Features:
                     Feature Description          Installed
-------------------------------------------------------------
```

Support for the additional MPs begins immediately. You do not need to restart the MX to place the upgrade into effect.

System Parameter Support

Table 1– 4, **Table 1– 5**, and **Table 1– 6** list the recommended or maximum supported values for major system parameters.

Table 1– 4. Mobility System Parameters

Parameter	Supported Value
MX switches in a single Network Domain	500
MX switches in a single Mobility Domain	64
Roaming VLANs per MX	❑ MX-2800: 256 total (256 configured) ❑ MX-400: 256 total (128 configured) ❑ MX-200/216: 256 total (128 configured) ❑ MX-8: 256 total (128 configured) ❑ MXR-2: 256 total (128 configured)
VLANs per Mobility Domain	2048
MPs per MX	❑ MX-2800: 4096 configured, 512 active ❑ MX-400: 480 configured, 120 active ❑ MX-200: 768 configured, 192 active ❑ MX-216: 768 configured, 192 active ❑ MX-8: 48 configured, 12 active ❑ MXR-2: 16 configured, 4 active Includes directly attached MPs and Distributed MPs. Inactive configurations are backups.
Minimum link speed between MXs in a Mobility Domain	128 Kbps
Minimum link speed between an MX and AP in a Mobility Domain	128 Kbps and 95ms round trip latency

Table 1– 5. Network Parameters

Parameter	Supported Value
Forwarding database entries	❑ MX-2800: 32768 ❑ MX-400: 16383 ❑ MX-200: 8192 ❑ MX-216: 8192 ❑ MX-8: 8192 ❑ MXR-2: 8192
Statically configured VLANs	❑ MX-2800: 256 configured ❑ MX-400: 128 configured ❑ MX-200/216: 128 configured ❑ MX-8: 128 configured ❑ MXR-2: 128 configured
Spanning trees (STP/PVST+ instances)	64
ACLs	ACEs per MX ❑ 170 ACEs per ACL: ❑ MX-2800: 256 ❑ MX-400: 256 ❑ MX-200: 256 ❑ MX-216: 256 ❑ MX-8: 25 ❑ MXR-2: 25
Location Policies	Location Policies per MX: All models: 1 The Location Policy can have up to 150 rules.
IGMP streams	500 **Note:** Replication of a stream on multiple VLANs counts as a separate stream on each VLAN.
Mesh Services and Bridging	❑ Mesh Depth — 3 Mesh Links (Portal<->Mesh MP<->Mesh MP) ❑ Mesh Fan Out— 6 APs ❑ Maximum Supported Mesh Nodes per Mesh Portal — 6 ❑ Bridge Links — 1:1

Table 1– 6. Management Parameters

Parameter	Supported Value
Maximum instances of RingMaster simultaneously managing a network	3
Telnet management sessions	❑ MX-2800: 8 ❑ MX-400: 8 ❑ MX-200: 8 ❑ MX-216: 8 ❑ MX-8: 4 ❑ MXR-2: 4 The maximum combined number of management sessions for Telnet and SSH together is 8 for the MX-400, MX-200, and MX-216, or 4 for the MX-8 and MXR-2, in any combination.
SSHv2 management sessions	❑ MX-2800: 8 ❑ MX-400: 8 ❑ MX-200: 8 ❑ MX-216: 8 ❑ MX-8: 4 ❑ MXR-2: 4
Telnet client sessions (client for remote login)	❑ MX-2800: 8 ❑ MX-400: 8 ❑ MX-200: 8 ❑ MX-216: 8 ❑ MX-8: 4 ❑ MXR-2: 4
NTP servers	3
SNMP trap receivers	8
Syslog servers	4
RADIUS and LDAP servers	40 configured on the MX 4 in a server group 4 server groups in a AAA rule A maximum of 40 servers in any combination of RADIUS and LDAP - for example, 30 RADIUS servers and 10 LDAP servers.

Table 1– 7. Client and Session Parameters

Parameter	Supported Value
Authenticated and associated clients per radio	100 Clients who are authenticated but not yet associated are included in the total.
Active clients per radio	50 Total number of active clients simultaneously sending or receiving data.

Table 1– 7. Client and Session Parameters (continued)

Parameter	Supported Value
Active AAA sessions (clients trying to establish active connections) per MX	❑ MX-2800: 12800 ❑ MX-400: 2500 ❑ MX-200: 4800 ❑ MX-216: 4800 ❑ MX-8: 300 ❑ MXR-2: 100
AAA users configured in local database	❑ MX-2800: 1000 ❑ MX-400: 999 ❑ MX-200: 999 ❑ MX-216: 999 ❑ MX-8: 250 ❑ MXR-2: 250

Known Behaviors and Issues

The following issues are known behaviors and issues in this version of Mobility System Software.

- When command auditing is enabled on the MX, the log file becomes too large and you cannot upgrade to new MSS versions. (66266, 66050)

  Description — Configuring the command audit log file size does not work as expected and the log file becomes too large for the flash memory. If you attempt to upgrade to a new MSS image using RingMaster, the error message "Download image Fail" is displayed. If you upgrade using the CLI, the error message "Not enough space available" is displayed during the TFTP process.

  Workaround — Delete all of the "log:command_audit.log" files from the flash memory of the MX. This allows you to perform the upgrade to the newer MSS image.

- Auto-tune channel-config lockdown feature does not work in a cluster configuration. (62746)

  Description: When operating in Cluster mode, the auto-tune channel lockdown command is not available.

  Workaround: None. Auto-tune lockdown must be completed via alternate mechanisms. e.g. RingMaster or auto-tune lockdown while in a basic Mobility Domain configuration.

- Mesh APs do not boot if a VLAN is configured with a VLAN tag. (58198)

  Description — If you configure Mesh APs with a VLAN tag, the AP does not boot using the auto boot-configuration feature.

  Workaround — Do not configure Mesh APs with VLAN tags.

- Voice handsets can be sensitive to changes on an in-service SSID. (41603)

  Description — Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information.

  Workaround — When using affected handsets, disable the Service Profile prior to making any configuration changes.

Issues Resolved Since Version 7.1.6.3

- You could not disable the WMM setting when using MSS to configuring VoIP handsets. (66888)
- The MX was unaccessible via the CLI until the MX was rebooted. (66826)
- The FakeAP alarm and counter was not generated when attempting to simulate a FakeAP attack. (66699)
- Configuring frame aggregation for 802.11n APs caused delays on the network especially for Intel 802.11n clients. (66651)
- The DFS algorithm was not working correctly in certain locations and on legacy MPs when an 11a radio is a single mode radio.(66599)
- Using the command show ap status all did not display all of the APs on the network. (66308)
- For the command, set radio-profile profile-name auto-tune, the option power-lockdown is deprecated and no longer available. (66307)

- The SIP-aware feature was not working as expected. (66294)
- When using WebPortal Local Switching on a network with MP-82s, clients repeatedly connected and disconnected on the network. (66270)
- When the cluster feature was configured on a network, the show ap command did not display all of the MPs with “up” status. (66247)
- After removing a client from the Black List and then adding the same client to the Black List caused the MX to be unresponsive on the network. (65788)

Issues Resolved Since Version 7.1.5.7

- When using Web Portal and connecting to the login page, the MP rebooted on the network. (65436)
- Performance issues for bridge and mesh configurations when using 802.11n modes are resolved. (64965)
- Upgrading from an earlier version of MSS 7.1 invalidated the existing certificates on the MX. (64640)
- If MP had vlan-tagging enabled, it did not boot in bridging mode. (61935)
- Some cluster configuration changes on the MX were not accurately reflected by RingMaster. (59864)

Issues Resolved Since Version 7.1.5.4

- If a non-802.11n MP has a service profile configured with the option to require 11n, the MP does not beacon SSIDs over the network. (65362)
- Mesh APs were timing out on the network. (64302)
- The time on the MX was drifting from the actual time on the network. (64156)
- When upgrading from an earlier version of MSS, CA certificates were deleted from the configuration. (63866)
- Some SSIDs were erroneously classified as rogue SSIDs on the network. (63829)
- The link up/down events on switch ports connected to the MP-82 were affecting connectivity to the network. (63144)

Changes to Default Behaviors in MSS

- The "dfs_channels" attribute in the radio profile of the Mesh AP backhaul radio must be enabled during pre-staging so that the backhaul link can be established on DFS channels. Please note that when there is no radio profile is specified, default radio profile is used. (63901)

Documentation Errata

- The ACL edit buffer is meant to be used for creating and editing one ACL at a time. If you need to create multiple ACLs, use '`commit security acl all`' after each ACL. This is not fully documented in the MSS User's Guide. (61703)

- Starting with 7.0, the dot1x reauth-period works only on a dynamic WEP and WPA with WEP-40 or WEP-104 cipher. In case that both the dot1x reauth-period and session-timeout attribute (from the service profile or RADIUS) are set, the session-timeout attribute value is used.

- Additional LDAP Command - the following command was added to the LDAP feature: (64054)

  - `MX# set ldap prefix-dn` ***`prefixdn`***

    The attribute, `prefixdn`, can consist of up to 64 characters with a default value of `cn`. It is the first RDN attribute name to be used during simple-authentication.

- The MSS User's Guide omits the information that configuring 11n means that TKIP and WEP are no longer configurable as encryption methods.

- Although not explicitly stated in the MSS User's Guide, mesh configuration is supported for 802.11n products including the MP-432, MP-82, and the MP-632.

- In addition to configuring the MP LED mode for a single MP, you can also configure the mode for a range of MPs and on auto MPs. Use the following commands:

  `MX# set ap` ***`apnumrange`*** `led-mode {auto|static|off}`

  `MX# set ap auto led-mode {auto|static|off}`

  Trapeze MPs and the equivalent OEM MPs are supported, however, the MP-71, MP-620, and MP-622 are not supported.

  The `blink` command takes precedence over the `led-mode` command.