



PowerEdge MX7000 Reset to Default

Technical Note by:

Sylvia Tien
Madhu Narasappa

SUMMARY

This 3 page technical paper discusses the “Reset to Default” feature found in Dell’s new PowerEdge MX7000 chassis. Also outlined are the front panel configuration storage options.

In this paper, we will outline all of the settings that are reset when a user performs a reset to defaults on the MX7000 chassis. Additionally, we describe the settings that are stored in the front panel so that users can understand what settings will need to be re-applied when management modules are replaced.

Reset to Default

Users can initiate a reset to defaults operation from either the racadm CLI utility, or via a REST API call to the management module. See below for the details on each of these.

During the reset configuration operation, the management module reboots, wipes out applicable configuration and restores them to the factory default values. Detailed information of reset configuration success/failures are logged in hardware logs (See CMC8731/CMC8732 in the Dell Message Registry). After a reset operation, you will always see the reset to defaults logged.

The Dell EMC MX7000 chassis supports a “Multi Chassis Management” (MCM) feature, which allows a stack of chassis that have been physically cabled together to be managed through a single management module.

Lead Chassis: If a chassis is lead chassis of a MCM group, then you must dissolve the MCM group before performing reset to default. The command will fail if you attempt to reset to defaults in an MCM Lead setup and an error message will return. *Error Message:* “Reset to defaults is not supported on a lead chassis in the MCM group.”

Member Chassis: If a chassis is member chassis of a MCM group, reset configuration is supported. However, chassis will be removed from the MCM group after the operation and become a standalone chassis.

Standalone Chassis: Reset configuration is fully supported for standalone chassis.





Resettable Management Module Configuration

This is a comprehensive list of configuration items which are impacted when a reset to default function is performed

- User Configuration
 - *Reset root password to factory shipped default password*
- Identity Configuration
 - *Reset chassis to default brand*
- Web SSL Certificate
 - *Re-generate web SSL certificate and key*
- Firewall configuration
 - *Reset firewall configuration to default*
- SNMP and SSH related configurations
- Network Configuration Settings
 - *Reset IPv4, IPv6, DNS, VLAN settings to defaults*
- Other User Configurable Settings
 - *Reset below settings to defaults*
 - Chassis Power Settings
 - Chassis Settings – Asset Tag, Chassis Name
 - Chassis Topology Settings
 - KVM Setting - Enable
 - LCD Settings
 - Network Switch Settings
 - Quick Sync Settings
 - Security Settings – Customer Certificate, Private Key
 - Serial Settings
 - Time Settings

Resettable Management Module Logs

- Hardware logs
- OpenManage Enterprise (OME) Modular logs
- Dumplog logs

Interfaces

To perform a reset to defaults, use one of the following interfaces:

1. [Redfish API](#)

URI: `api/ApplicationService/Actions/ApplicationService.ResetApplication`

JSON Payload:

```
{ "ResetType": "<ResetType value>" }
```

Supported ResetType values:

- RESET_CONFIG: Reset resettable management module configuration mentioned above
- RESET_ALL: Reset resettable management module configuration and logs mentioned above
(RESET_ALL = RESET_CONFIG + logs)



Interfaces cont.

2. Racadm

The CLI racadm command is equivalent to Redfish API ResetType of RESET_CONFIG.

- racadm racresetcfg

Locked Management Module Configurations

Reset configuration with types of RESET_CONFIG and RESET_ALL will not reset these management module configuration settings:

- Chassis MAC Addresses
- Chassis Service Tag
- Factory Shipped Default Password
- Identity Certificates

Management Module Configuration Persistence

Management module configuration data persist through system boots and failovers. Some configuration settings persist through management module card replacement because they are stored in nonvolatile flash memory located in chassis right control panel. If the right control panel is replaced, the current management module configuration is lost and the system will assume the management module configuration in the new right control panel. If the new right control panel has not been configured or has been performed reset to defaults, new management module configuration will use the default factory values.

Below configurations persist through management module card replacement:

- Root Password
- Branding ID Module
- Network Configuration Settings (as listed above)
- Other User Configurable Settings (as listed above)
- Hardware Logs
- Chassis MAC Addresses
- Chassis Service Tag
- Factory Shipped Default Password

Conclusion

Periodically it might be necessary to reset a chassis and in this paper we discussed the methods and interfaces to perform reset to factory defaults, along with a listing of the settings that are reset, and settings that are not impacted. The retention of some persistent storage of the critical chassis information on the chassis right control panel, and which settings are retained in case of management card replacement mean that they reduce risk and increase chassis availability.