Dell Open Server Manager built on OpenBMC™ 3.0.0 User's Guide

July 2024
Rev. A00

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

About Dell Open Server Manager (OSM) built on OpenBMC™

Dell Open Server Manager (OSM) built on OpenBMC™ is a Dell implementation of OpenBMC for PowerEdge servers. OpenBMC is a Linux Foundation project to produce an open-source Baseboard Management Controller (BMC) firmware stack that is designed to run across heterogenous infrastructure. OpenBMC allows you to remotely monitor, manage, and control a server. OpenBMC is useful if you want consistent system management across different infrastructure, while maintaining code transparency for security validation and trust. Open Server Manager is a Dell project that is designed, tested, and validated to securely run OpenBMC on select PowerEdge platforms.

Topics:

Key features

The key features of Open Server Manager 3.0.0 include:

- View server health
- View hardware inventory
- View sensor information such as temperature and voltage
- View memory information
- Monitor and control power usage
- View and configure network management settings with IPv4 and IPv6 (Redfish only) support
- Virtual consoles with virtual media support
- Perform power-related operations such as graceful restart and power cycle
- Monitor and limit power consumption
- Log event data
- Signed firmware updates
- Role-based authorization
- Default login password modification
- Generate TSR collection for Dell support
- Redfish supports only:
  - Virtual AC chassis power cycle
  - PCIe network adapter operations
  - NVMe (must support basic management) drive status
  - BIOS settings configuration using Server Configuration Profiles (SCP)
- User authentication through Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) Directory Service, or locally administered user IDs and passwords

2

Get Started with Open Server Manager

Topics:

Prerequisites

Ensure that Open Server Manager is enabled at the factory and shipped with the server. Open Server Manager must be installed and running on the BMC.

Open Server Manager supports the following PowerEdge servers:

- PowerEdge R670 CSP Edition
- PowerEdge R770 CSP Edition

License

A license is required to enable Open Server Manager on the server. The license is perpetual for the life of the server and enables all features.

Log in to Open Server Manager

1. In the address bar of a supported web browser, enter **https://<IP Address>** of the BMC that you want to connect to.
2. From the Open Server Manager login to window, enter the **Username** and **Password**.
3. Click **Log in**.

   NOTE: The default username is **root** and the default password is **0penBmc**. However, it is mandatory to change the username and password of your choice after your login with default credentials. The first character in the password is a zero. Click **Profile settings** to view your username and change your password.

Restore the server using the Easy Restore feature

The Easy Restore feature restores the server service tag and BIOS or OSM configuration data after replacing the DC-SCM (Data Center Security Control Module). System configuration data is automatically maintained in a backup flash device within the system. If the BIOS detects a new DC-SCM module during server boot, the system prompts the user to restore the backup system configuration data.

The following system configuration data is restored:

- BIOS—All configuration settings

OSM:

- NTP server settings
- Network settings
  - Domain name and hostname settings
  - DNS and NTP server settings
  - DHCP settings

    - Enable or disable USB NIC settings
- User account policy settings
- Access policy to enable the BMC shell using SSH
- Power restore policy
- Server power operation access

The following OSM settings are not restored and reset to default values:

- Local users—After Easy Restore, only the **root** user are available with the password **0penBmc**. Users are required to change the root password at the next login.
- Static IPv4 and IPv6 addresses—Network settings are reset to use DHCP
- LDAP authentication configuration settings
- User SSL certificates
- Access policy to enable IMPI over the network
- Server power boot settings for one-time boot
- System identify LED settings

3

View system information

You can view Open Server Manager managed system and status information.

Topics:

Overview

When you log in to the OSM UI, the **Overview** page is displayed. On this page, you can view the following:

- **BMC time**—Displays the BMC time in the time zone of the user, which is determined by the web browser.
- **SOL console**—Launches the Serial over LAN (SoL) console.

System Information:

- **Server information**—Displays the information of the server.
- **Network information**—Displays the BMC network settings.
- **Firmware information**—Displays the BMC and server firmware information.

Status Information:

- **Event Logs**—Displays any critical and warning events.
- **Inventory and LEDs**—Turn on or turn off the system identify LED.

You can click **View more** to view and edit more information about System and Status information.

You can also click **Health** button on the upper right corner of the page to view the **Event logs**.

Click **Power** button on the upper right corner of the page to view **Server Power Options**.

Click **Refresh** to refresh the information about the dashboard.

Click the username in the upper right corner of the page and then click **Profile settings** to view your username, change your password, and set the time zone display preference.

Click **Log out** to log off from the system.

4

Manage Logs

Open Server Manager provides events logs related to the server such as power events, firmware updates, configuration changes, hardware changes, or issues. You can apply filters to the logs and can export the entire log to a location on your system.

Topics:

Event log

When a system event occurs on a managed system, it is recorded in the System Event Log (SEL). You can view and filter event log files from the Open Server Manager.

From the Event Log page in the UI, you can perform the following actions:

- Search through event logs by entering keywords and clicking **Search.**
- Filter the event logs by severity (OK, Warning, and Critical) and status (Resolved and Unresolved). You can select multiple severity land status levels.
- Filter the event logs by date range.
- Select multiple event logs by clicking the checkbox next to event log. After you select the event logs, you can delete the logs by clicking **Delete All** and then clicking Yes in the confirmation message or you can also mark event logs as Resolved. You can also click **Export all** to export your selected logs to your system.

SupportAssist

Open Server Manager helps you generate a SupportAssist collection that is known as Technical Support Report (TSR) of the server and then export the collection to a location on the local management station.

To generate the SupportAssist collection manually:

1. On the **Event log** page of the UI, in the SupportAssist section, select the log type as **TSR Full**, **TSR PII Removed, Inventory Full,** , or **Inventory PII Removed**. By default, TSR Full logs are collected if you do not select any log type and run export log.
2. Click **Export Log** . A message is displayed indicating that **Log Collection Started**. You must wait till the log collection is completed.
3. After the log collection is completed, **SupportAssist Download Ready** dialog box appears.
4. Click **Download**. When prompted, you can either open the SupportAssist.zip file or save it locally. If you select **Save**, you can save the file in any location.

POST code log

POST codes are progress indicators from the system BIOS, indicating various stages of the boot sequence from power-on-reset. It also enables you to diagnose any issues that are related to system boot.

NOTE: You cannot clear POST code logs from the web UI. POST code logs can be cleared using the only Redfish interface.

On the POST code log page in the web UI, you can perform the following actions:

- Search through POST code logs by entering keywords in the **Search** box.
- Filter the POST code logs by a date range.
- You can also click **Export all** to export your selected logs to your local system.

5

View Hardware Status

Under the Hardware status menu in the UI, you can view the hardware status of various hardware components in your server.

You can view data about the following hardware components:

- System
- BMC manager
- System components and peripherals (chassis)
- Memory (DIMM slots)
- Processors
- Fans
- Power Supply Units (PSUs)

You can also view the associated events of all hardware in the server.

Topics:

View Inventory and LEDs

On the Inventory and LEDs page in the web UI, you can view the hardware components and their status.

You can click the toggle switch to either **Off** or **On** to turn on or turn off the system identify LED.

NOTE: Toggle switch is only supported to the system itself.

You can view the status of hardware components in your server. Click any of the hardware components and expand the view for more information.

NOTE: Inventory information is queried from the Field Replaceable Unit (FRU) inventory device data that is returned by the component itself, and may not support all available properties.

You can use the search feature to get information for specific hardware components.

View sensors

View all the sensors that are available in the system.

On the Sensors page in the web UI, you can do the following:

- Search and filter for specific sensors by using the **Search** feature.
- Filter sensors by severity (OK, Warning, or Critical).
- You can export sensor details for one or multiple components.

NOTE: The Open Server Manager web UI shows only the threshold sensors. A complete list of all sensors can be queried from IPMI.

6

Manage Operations

Under the Operations menu in the UI, you can perform the following tasks:

- **KVM**—Start the virtual Keyboard, Video, and Mouse (KVM) console.
- **Firmware**—Update the BMC and server firmware.
- **Reboot BMC** —Restart the BMC and view the current BMC boot status.
- **Serial over LAN console**—View information over the serial port of the server.
- **Server power operations**—View the current server status and perform server power operations.
- **Virtual media**—Attach image files as virtual media devices on the server.

Topics:

Manage KVM

Open Server Manager includes an enhanced HTML5 virtual KVM over the standard VNC client. Use the virtual console to manage a remote system using the keyboard, video, and mouse on your management station to control the corresponding devices on a managed server.

You can start the KVM console on the KVM page in the UI to interact with the remote system.

Update Firmware

You can update server components using the firmware update feature. The Dell Update Package (DUP) functionality can be used to update server components on Open Server Manager enabled Dell servers. Firmware updates can be done through the Open Server Manager web UI or Redfish interface.

NOTE: Updating to iDRAC firmware from OSM version 3.0.0 is not supported.

1. Select **Add file** to browse locally for the firmware image you want to apply.
2. Select **Upload** to upload the firmware image.
   A message is displayed stating that the upload has started. The upload process may take one minute depending on the size of the DUP image file.

   NOTE: The version of the firmware being uploaded must not be the same version as any running firmware or backup firmware image already installed.

   After you verify that the image file is successfully uploaded, a message is displayed. The updated version is displayed in the Uploaded Image section of the device.
3. Select **Activate** to update the firmware or **Delete** to remove the uploaded image file.
   When prompted, select accordingly to indicate if you want to install now or later.

   NOTE:
   - For devices that do not require a reboot to update, only the Now option is displayed.
   - For devices that require a reboot, selecting Now automatically restarts the server and runs the update. If you select later, the firmware is updated after the server is restarted next time.
4. After the update process starts, view the Event Logs to monitor the update process.

   If the update is successful, you see the updated firmware version running for the device being updated.

NOTE: The previous image which was listed under **Running**, now is listed under **Backup**, and the previous Backup image file is deleted.

5. If the update is unsuccessful, the "Running" and "Backup" images are not changed, and an option to delete the unsuccessful image file is displayed.

Table 1. Firmware update—Supported components

Component Name	Firmware Rollback Supported? (Yes or No)	Out-of-band—System Restart Required?	In-band—System Restart Required?
Open Server Manager	Yes	No	No
BIOS	Yes	Yes	Yes
CPLD	Yes	Yes	Yes
Backplane (SEP)	Yes	No	No
FLOPCPLD	Yes	Yes	Yes

Restart BMC

1. In the right pane, expand **Operations**.
2. Click **Reboot BMC** > **Reboot BMC**.

NOTE: Resetting the BMC to the default settings is not supported in the web UI. It is only supported through the Redfish interface.

Serial over LAN console

You can launch the Serial over LAN (SoL) console that displays the output of the serial port of the server.

Restart the server

To update the system boot preference, select the boot setting override type from the **Boot setting override** menu. By default, **Enable one time boot** is selected automatically.

1. To reboot the server, select the type of reboot from **Operations** > **Reboot server**.
   - Orderly—The operating system shuts down first, and then the server restarts.
   - Immediate—Select to immediately restart the server. However, if you restart the server without shutting down the operating system, data may be corrupted.
2. Click **Reboot**.

Shut down the server

1. To shut down the server, select the type of shutdown from **Operations** > **Shutdown server**.
   - Orderly—The operating system shuts down first, and then the server reboots.
   - Immediate—Select to immediately restart the server. However, if you restart the server without shutting down the operating system, data may be corrupted.
2. Click **Shutdown**.

NOTE: After an orderly shutdown or restart server operation is sent to the host device, it is up to the host device to support that request and perform it.

Start a virtual media session

Media image files (ISO or IMG) are displayed as media devices attached to a server.

You can:

- Remotely access media connected over the network.
- Install the applications.
- Update the drivers.
- Install an operating system on the managed system.

1. Under **Virtual media device**, click **Add file**.
2. Select the file and click **Open**.
3. Click **Start**.
4. To disconnect the virtual media device, click **Stop**.

NOTE:

- After you click the **Start** button to attach the virtual media image file, you will no longer see the attached image file in the web UI.
- After attaching a virtual media image file, refreshing the browser web page may detach the virtual media image file.
- The Open Server Manager webserver timeout value is 30 minutes (fixed value). Virtual media images are automatically detached when the timeout is exceeded.

7

Manage settings

Topics:

Set BMC date and time settings automatically

NOTE: The BMC default time is in UTC format.

1. In the right pane, expand **Settings**.
2. Click **Date and time** > **NTP**.
3. Enter the NTP server address.

   NOTE: Open Server Manager supports adding up to three NTP servers.

4. Click **Save setttings**.

Set date and time settings manually

1. In the right pane, expand **Settings**.
2. Click **Date and time** > **Manual**.
3. Enter the date and time.
4. Click **Save setttings**.

   NOTE:
   - If you want to change how the time is displayed (either UTC or CDT UTC-5), go to **Profile Settings** > **Timezone Display Preference**.
   - If you manually change the date or time and you reboot the server, Open Server Manager updates the BMC date and time from the BIOS.
   - The default date and time is manually set to the time that the firmware was built in UTC format.

Configure Network Settings

On the Network page in the web UI, you can view the BMC network configuration, edit the system hostname, and toggle the use of a domain name, DNS servers, and NTP servers.

- Special characters are not allowed for hostnames, except for the hyphen (-) character.
- The mgmt0 interface represents the rear dedicated management port of the server. On PowerEdge servers with cold-aisle serviceability (front I/O configuration), the mgmt0 interface bonds both the front and rear dedicated management ports. In this configuration, the front dedicated management port is the primary management port.
- If both the front and rear dedicated management ports are connected to the network in the cold-aisle configuration, ensure that both ports are connected to the same network and subnet to avoid network connectivity issues.
- Setting an invalid gateway for mgmt0 ends the connection to both mgmt0 and other shared management network interfaces. To open the Device Settings page and configure the mgmt0 network interface, press F2.

- By default, the shared management network interfaces (NC-SI) are disabled. To use these interfaces, enable the interface by setting the property `{"InterfaceEnabled" : true}` using Redfish for the particular interface. These interfaces are available as **ensX** on the Network page where X represents the slot in which the corresponding OCP card is plugged-in.

Add a static IPv4 address

1. Select the correct Ethernet interface: **(mgmt0, ensX)**.
2. Click **Add static IPv4 address**.
3. Enter the data in the **IP address**, **Gateway**, and **Subnet mask** fields.
4. Click **Add**.

NOTE:

- You can delete any IPv4 address by clicking the delete icon.
- Adding static IPv4 does not automatically disable DHCP on the interface. To disable DHCP, toggle the DHCP button on the Network page for the interface.

Add a static DNS address

1. Select the correct Ethernet interface: **(mgmt0, ensX)**.
2. Click **Add IP address**.
3. Enter the IP address of the **Static DNS**.
4. Click **Add**.

NOTE:

- You can delete any DNS address by clicking the delete icon.
- The LinkStatus property always indicates that the link is working even if the cable is disconnected.
- The default setting for all network interfaces is DHCP.
- You can disable a network interface only using Redfish.

Manage USB NIC

The USB NIC is used to manage OSM from the host operating system.

- To enable the USB NIC feature, set the toggle switch to **Enabled**.
- To disable the USB NIC feature, set the toggle switch to **Disbaled**.

8

Manage security and access

Topics:

View sessions

On the Sessions page in the web UI, you can view user sessions that are connected to the system.

NOTE: SSH sessions to Open Server Manager do not get reported as active sessions.

NOTE: SSH sessions to Open Server Manager provide a restricted ipmitool shell that only accepts known IPMI commands. The `obmc-console-client` command initiates a host serial redirect session.

You can view the user session information in the table. To view the user sessions:

1. You can search for sessions by using the **Search**box.
2. To disconnect any session, click **Disconnect**. You can also select multiple sessions to disconnect.

LDAP

Enable LDAP authentication

On the LDAP page in the web UI, to enable LDAP authentication, do the following:

1. Select the **Enable** check box.

   NOTE: Select the **Enable** check box if you want to secure LDAP using Secure Socket Layer (SSL). You must have a CA certificate and an LDAP certificate to enable secure LDAP.

2. Select either **Open LDAP** or **Active directory** as the service type.
3. Enter the required information.
4. Click **Save settings**.

Add a role group

1. Enter a name for the role group.
2. Click **Add role group**.
3. Set the privilege of the role group to **Administrator**, **Operator**, **User**, or **NoAccess (Callback)**.
4. Click **Save**.

Remove a role group

1. Select the check box next to the role group or groups that you want to remove from the table.
2. Click **Remove role groups**.

3. When prompted, click **Remove**.

Modify the privileges of a role group

1. Select the check box next to the role group or groups that you want to modify from the table.
2. Click the **Edit** icon.
3. Change the privilege of the role group to **Administrator**, **Operator**, **User**, or **NoAccess (Callback)**.
4. Click **Save**.

User Management

You can set up user accounts with specific privileges (role-based authority) within Open Server Manager. By default, Open Server Manager is configured with a local administrator account. As an administrator, you can set up user accounts to allow other users to access Open Server Manager.

Add a user

1. Click **Add user**.
2. Set the account status to either **Enabled** or **Disabled**.
3. Enter a new username.

   NOTE:
   - The username can start with a lowercase letter, a number, a dot, or the following symbols—@, $, (,).
   - The middle letters can contain lowercase letters, numbers, a dot, or the following symbols—_, $, (,), \, ~, -.
   - The username can end with a lowercase letter, number, a dot, or the following symbols—_, $, (,), ~, -.
   - The username cannot start with a number.

4. Set the privilege of the user to **Administrator**, **Operator**, **ReadOnly**, or **NoAccess (Callback)**.
5. Enter the password of the user.

   NOTE:
   - Password strength and requirements are governed using the PAM cracklib module.
   - Passwords are required to be between 8 and 20 characters long, inclusive.
   - Passwords must not contain common dictionary words as defined by a local version of cracklib-small2 on the BMC.
   - Passwords must not be palindromes (identical backwards and forwards) even if they are not a dictionary word. For example, 1aeioiea1 and racecar are considered palindromes.
   - Passwords cannot contain the username being modified directly or reversed.

6. Reenter the password for confirmation.
7. Click **Add user**.

Delete a user

1. Click the check box next to the user or users that you want to remove from the table.
2. Click **Remove** > **Remove** .

Modify user settings

1. Click **edit** to modify the user settings by selecting the user from the table.

   You can now update the following properties:
   - Maximum failed login attempts—Change the number of allowed failed login attempts.
   - User unlock method—Set to **Automatic after timeout** or **manual**.

NOTE:

- In the **Automatic after timeout** unlock setting, after the lockout timeout starts for a user, if the user tries to log in again during the timeout duration the lockout timer restarts.
- Only non-root accounts can be locked.

2. You can also select the check box next to a user account, to enable, disable, or delete the user.
   You can view the following privilege role descriptions by clicking **View privilege role descriptions**.

Table 2. Privilege Role Descriptions

Role	Privilege
Administrator	Log in, Configure, Configure Users, Logs, System Control, Access Virtual Console, Access Virtual Media, System Operations, Debug
Operator	Log in, Configure, System Control, Access Virtual Console, Access Virtual Media, System Operations, Debug
ReadOnly	Login
NoAccess	None

Policies

On the Policies page of the UI, you can enable or disable the system policies.

- **BMC shell (via SSH)**—Allows access to Shell sessions through SSH. Use the toggle switch to enable or disable the policy.
- **Network IPMI (out-of-band IPMI)**—Allows remote management of the platform by using the Intelligent Platform Management Interface (IPMI). Tools such as the ipmitool require this setting to be enabled. Use the toggle switch to enable or disable the policy.

NOTE:

- When you disable or enable IPMI or SSH, the changes are reflected in the web UI after 15 s to 20 s. If you refresh the page before then, you may see the previous settings. After 15 s to 20 s, the page will update and display the current settings.
- Network IPMI is supported only on the dedicated management interface.

Certificates

Generate a Certificate Signing Request (CSR), add new certificates, and replace existing certificates.

Generate a CSR

1. Click **Generate CSR**.
2. Enter the required data under the **General** section.
3. Under **Private key** > **Key Pair Algorithm**, select the algorithm as **EC** or **RSA**.

   NOTE: If you select **Key Pair Algorithm** as **EC**, you can select any **Key Curve Id** from the drop-down menu. If you select **Key Pair Algorithm** as RSA, then select **Key Bit Length** as 2048.

4. Click **Generate CSR**.

Add a certificate

1. Click **Add new certificate**.
2. Select the certificate type as **LDAP Certificate** or **CA Certificate**.
3. Click **Choose file** > **Open** > **Replace**.

Delete a CA certificate

1. Select the CA certificates that you want to remove from the table.
2. Click the delete icon.
3. When prompted, click **Delete**.

NOTE:

- CA certificates can be removed using the **Delete** option.
- LDAP certificates cannot be removed using **Delete** option. Instead, reset the BMC to default settings to remove the certificate.
- HTTPS certificates cannot be removed.

9

Manage the system using IPMI

The following section describes how to configure and manage your system by using the Intelligent Platform Management Interface (IPMI).

Topics:

IPMItool

You can use the IPMItool to control the BMC over IPMI through Open Server Manager. IPMItool is a utility to monitor, configure, and manage devices that support IPMI.

NOTE: OSM does not support IPMI `delloem` commands.

IPMI commands

Table 3. Sensor operations using IPMI

Command	Description	Syntax
SDR list	Displays sensor data repository (SDR) entry readings and their status	`ipmitool sdr`
SDR extended list	Displays extended sensor information	`ipmitool sdr elist`
SDR get	Displays information for specific sensors that are specified using sensor ID	`ipmitool sdr get <sensor name>`
SDR type	Displays all sensors for a given sensor type	`ipmitool sdr type <sensor type>`

Table 4. SEL operations using IPMI

Command	Description	Syntax
SEL clear	Clears the contents of the System event log	`ipmitool sel clear`
SEL elist	Displays extended information from the System event log	`ipmitool sel elist`
SEL list	Displays information from the System event log	`ipmitool sel list`

Table 5. User Management using IPMI

Command	Description	Syntax
user summary	Displays a summary of user ID information including maximum number of user IDs, the number of	`ipmitool user summary <channel number>`

Table 5. User Management using IPMI (continued)

Command	Description	Syntax
	enabled users, and the number of fixed names defined.	
user list	Displays a list of user information for all defined user IDs	`ipmitool user list <channel number>`
user set name	Sets the username that is associated with the given user ID.	`ipmitool user set name <user id> <username>`
user set password	Sets the password for the given user ID. If no password is given, the password is cleared.	`ipmitool user set password <user id> [<password> [<16|20>]]`
user enable	Enables access to the BMC for the given user ID.	`ipmitool user enable <user id>`
user disable	Disables access to the BMC for the given user ID.	`ipmitool user disable <user id>`

Table 6. Chassis operations using IPMI

Command	Description	Syntax
Power status	Displays power information regarding the high-level status of the system chassis and main power subsystem.	`ipmitool chassis power status`
Power on	Powers on the host	`ipmitool chassis power on`
Power off host	Powers off the host	`ipmitool chassis power off`
Power cycle host	Powers cycle the host	`ipmitool chassis power cycle`
Power reset	Restarts the host	`ipmitool chassis power reset`

Table 7. FRU operations using IPMI

Command	Description	Syntax
FRU print	Read all Field Replaceable Unit (FRU) inventory data and extract such information as serial number, part number, asset tags, and short strings describing the chassis, board, or product.	`ipmitool fru print`

10

Manage the system by using DMTF Redfish APIs

The systems from Open Manage Server can be managed by using the DMTF Redfish APIs.

Topics:

Overview

The Redfish Scalable Platforms Management API is a standard that is defined using the Distributed Management Task Force (DMTF). Redfish is a next-generation systems management interface standard, which enables scalable, secure, and open server management. It is a new interface that uses RESTful interface semantics to access data that is defined in model format to perform out-of-band systems management. It is suitable for a wide range of servers ranging from stand-alone servers to rackmount and bladed environments and for large-scale cloud environments. For more information about APIs, see the *Open Server Manager Redfish API Guide* available on Dell Technologies Developer.

URL Support

Redfish is a web-based API which implies that resources are accessed using client supplied URLs. URLs are required to identify the Redfish resources. The Redfish API uses a simple URL hierarchy which follows a /redfish/v1/ pattern for all the resources. The regular expression for a URI includes a trailing slash and is treated as a normative definition. However, Redfish service treats URIs with and without trailing slash as equivalent. Open Server Manager supports the following URI patterns:

- /redfish—URL for the Redfish version object.
- /redfish/v1—Root URL for version 1 of the Redfish services.
- /redfish/v1/odata—Redfish services expose an OData service document at this URI. This service document provides a standard format for enumerating resources that are exposed by the service by enabling all generic hypermedia-driven OData clients to go to the resources of the service.
- /redfish/v1/$metadata—Redfish services expose a metadata document in XML format. This document describes the resources and collections that are available at the service root URI. It also provides references to other metadata documents, which describe the complete set of resource types that are exposed by the service.
- /redfish/v1/$metadata#{Collection or a Singleton resource}—Metadata URL specified as a part of @odata.context property for all resources. This URL returns data in XML format.
- /redfish/v1/JsonSchemas/{JsonSchemaFileId}—This URL returns data in JSON format. The output is a collection of the JsonSchemaFile resource instances.
- /redfish/v1/JsonSchemas/{resource URI}—The JSON Schema File resource instance describes the location (URI) of a particular Redfish schema definition being implemented or referenced by a Redfish service. This URL returns data in JSON format.
- /redfish/v1/{other resource-specific URIs}—All instrumentation resources follow this pattern.

HTTP headers

In addition to the mandatory headers described in the Redfish specification, Open Manage Server supports the following request headers:

Table 8. Request Headers

Header	Behavior
Content-Encoding	Support gzip encoding for metadata URIs.
Content-Length	Mandatory on all responses except those having "Transfer-Encoding: chunked."
Content-Type	All URIs: charset=utf-8 shall be supported. All URIs except metadata requests: application/json is returned. For OData metadata requests (see $metadata below): application/xml is returned.
Location	Mandatory for all requests that create resources (for example session creation) and for redirecting HTTP requests to other resources (for example Tasks).

Redfish resources

Common System Management Actions

Open Server Manager Redfish APIs supports the following common functions.

Server Power Operations

Table 9. Server Power Operations

URI	/redfish/v1/Systems/system/Actions/ComputerSystem.Reset
Example	`curl -X POST -k https://${OSM}/redfish/v1/Systems/system/Actions/ComputerSystem.Reset -H "Content-Type: application/json" -u <OSM username>:<OSM password> -d '{"ResetType": "ForceOn"}'`
Allowable Values for ResetType	To get current supported values for the OSM version installed, run GET on URI `redfish/v1/Systems/system/ResetActionInfo`.

Reboot Open Server Manager

Table 10. Reboot Open Server Manager

URI	/redfish/v1/Managers/bmc/Actions/Manager.Reset
Example	`curl -X POST -k https://${OSM}/redfish/v1/Managers/bmc/Actions/Manager.Reset -H "Content-Type: application/json" -u <OSM username>:<OSM password> -d '{"ResetType": "GracefulRestart"}'`
Allowable Values for ResetType	To get current supported values for the OSM version installed, run GET on URI `redfish/v1/Managers/bmc/ResetActionInfo`.

Reset Open Server Manager

Table 11. Reset Open Server Manager

URI	/redfish/v1/Managers/bmc/Actions/Manager.ResetToDefaults
Example	`curl -X POST -k https://${OSM}/redfish/v1/Managers/bmc/Actions/Manager.ResetToDefaults -H "Content-Type: application/json" -u <OSM username>:<OSM password> -d '{"ResetType": "ResetAll"}'`

Table 11. Reset Open Server Manager (continued)

URI	/redfish/v1/Managers/bmc/Actions/Manager.ResetToDefaults
Allowable Values for ResetType	To get current supported values for the OSM version installed, run GET on URI `redfish/v1/Managers/bmc` and view ResetType@Redfish.AllowableValues property.

NOTE: This action resets the root password back to the default value '0penBmc'. You must change the default password before you run any Redfish actions. To change the root default password, see **Change Root Default Password** curl example.

Change Root Default Password

Table 12. Change Root Default Password

URI	redfish/v1/AccountService/Accounts/root
Example	`curl -X PATCH -k https://${OSM}/redfish/v1/AccountService/Accounts/root -H "Content-Type: application/json" -u root:0penBmc -d '{"Password": "<new string password>"}'`
Allowable Values for ResetType	New string password

Reset Chassis

Table 13. Reset Chassis

URI	/redfish/v1/Chassis/DELL_Baseboard/Actions/Chassis.Reset
Example	`curl -X POST -k https://${OSM}/redfish/v1/Chassis/DELL_Baseboard/Actions/Chassis.Reset -H "Content-Type: application/json" -u <OSM username>:<OSM password> -d '{"ResetType": "PowerCycle"}'` **NOTE:** • Once you perform the AC Power Cycle on the server, your server might power back on depending on the PowerRestorePolicy property current value. It is recommended to GET or PATCH this property before you AC cycle the server.
Allowable Values for ResetType	PowerCycle

OEM Actions

The following sections show the OEM actions that are supported through Open Server Manager Redfish APIs.

Export of the system configuration (BIOS only supported)

Table 14. Export of the system configuration (BIOS only supported)

URI	/redfish/v1/Managers/bmc/Actions/Oem/Dell/DellOpenBMCManager.ExportSystemConfiguration
Example	`curl -X POST -k https://${OSM}/redfish/v1/Managers/bmc/Actions/Oem/Dell/DellOpenBMCManager.ExportSystemConfiguration -u <OSM username>:<OSM password> -H "Content-Type: application/json`

There is no payload for this action but return as system configuration JSON document.

Import of the system configuration (BIOS only supported)

Table 15. Import of the system configuration (BIOS only supported)

URI	**/redfish/v1/Managers/bmc/Actions/Oem/Dell/DellOpenBMCManager.ImportSystemConfiguration**
Example	`curl -X POST -k https://<OSM IP>/redfish/v1/Managers/bmc/Actions/Oem/Dell/DellOpenBMCManager.ImportSystemConfiguration -u <OSM username>:<OSM password> -H "Content-Type: application/json" -i -d '{"SystemConfiguration":{"Comments":[{"comment":"Export type is Normal,JSON,Selective"}],"Model":"PowerEdge R650xs","Components":[{"FQDD":"BIOS.Setup.1-1","Attributes":[{"Name":"NumLock","Value":"On","Set On Import":"True","Comment":"Read and Write"},{"Name":"ErrPrompt","Value":"Enabled","Set On Import":"True","Comment":"Read and Write"}]}]}}'`

The payload for this request is the system configuration JSON to be uploaded to the Open Server Manager.

SupportAssist

Table 16. SupportAssist

URI	**/redfish/v1/Managers/bmc/Actions/Oem/Dell/DellOpenBMCManager.SupportAssistCollect**
Example for Remote connection	`curl -X POST -k https://${OSM}/redfish/v1/Managers/bmc/Actions/Oem/Dell/DellOpenBMCManager.SupportAssistCollect -H "Content-Type: application/json" -u <OSM username>:<OSM password> -d '{"ExportType": "TFTP", "Filter": "None", "ReportType": "TSR", "ExportTypeOptions": {"URI": "${SERVER_URL}"}}'`
Allowable Values for "ExportType" (string)	TFTP
Allowable Values for "Filter" (string)	• PII • None
Allowable Values for "ReportType" (string)	• Inventory • TSR
Allowable Values for "ExportTypeOptions" (complex type) • **Allowable Values for "URI" (string)**	Any valid URI

USB NIC

Table 17. USB NIC

URI	**/redfish/v1/Managers/bmc/Actions/Oem/Dell/DellOpenBMCManager.UsbNicEnable**
Example	`curl -X POST -k https://${OSM}/redfish/v1/Managers/bmc/Actions/Oem/Dell/DellOpenBMCManager.UsbNicEnable -H "Content-Type: application/json" -u <OSM username>:<OSM password> -d '{"UsbNicEnable":true}'`
Property "UsbNicEnable" (boolean) Allowable Values	Allowed values are true or false.