Dell EMC OpenManage Integration Version 1.1.0 with Microsoft Windows Admin Center

User's Guide

July 2020
Rev. A00

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

Overview of OpenManage Integration with Microsoft Windows Admin Center

Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) enables IT administrators to manage the PowerEdge servers as hosts, Microsoft Failover Clusters created with PowerEdge servers, and Hyper-Converged Infrastructure (HCI) created by using the Dell EMC Solution for Microsoft Azure Stack HCI (Storage Space Direct Ready Nodes or AX nodes). OMIMSWAC simplifies the tasks of IT administrators by remotely managing the PowerEdge servers and clusters throughout their life cycle. For more information about the features and benefits of OMIMSWAC, see the documentation at Dell.com/OpenManageManuals.

Key features of OMIMSWAC

- OMIMSWAC provides a simplified solution to IT administrators to efficiently manage the following:
  - Dell EMC PowerEdge servers running on supported Windows Operating Systems.
  - Azure Stack HCI clusters based on AX nodes or Storage Spaces Direct Ready Nodes from Dell EMC.
  - Microsoft failover clusters created with Dell EMC PowerEdge servers.
- View overall Health, Hardware inventory, and iDRAC inventory of nodes including component-level information of all supported Dell EMC platforms.
- Provides Update Compliance reports against Dell EMC verified update catalogs and notifications for new catalog versions.
- Support for different baselines in OMIMSWAC when connected to the Internet:
  - Dell EMC Enterprise Catalog for PowerEdge Servers.
  - Dell EMC Azure Stack HCI Solution Catalog for Dell EMC Solutions for Microsoft Azure Stack HCI.
  - Dell EMC MX Solution Catalog for PowerEdge MX Modular.
- Support for local baselines created using Dell EMC Repository Manager (DRM).
- Update PowerEdge Servers against baseline – BIOS, driver, firmware, and/or system management applications.
- Cluster-Aware Updating against validated baseline (BIOS, driver, firmware, and/or system management applications) for PowerEdge server-based Failover cluster and Dell EMC Solutions for Microsoft Azure Stack HCI.
- View iDRAC information of PowerEdge servers. For out-of-band management, you can directly launch the iDRAC console from Windows Admin Center.
- Availability of OMIMSWAC extension and documentation localized in English, French, German, Spanish, Simplified Chinese, and Japanese languages.

Topics:

New in this release

- Added support for Dell EMC Online Catalogs:
  - Dell EMC Enterprise Catalog for PowerEdge Servers.
  - Dell EMC Azure Stack HCI Solution Catalog for Dell EMC Solutions for Microsoft Azure Stack HCI.
  - Dell EMC MX Solution Catalog for PowerEdge MX Modular.
- Ability to perform Server update including selective component updates.
- Ability to perform Cluster-Aware Updating against validated baseline (BIOS, driver, firmware, and system management applications) on the following.
  - PowerEdge server-based Failover cluster
  - Dell EMC Solutions for Microsoft Azure Stack HCI

NOTE: For the Cluster-Aware Updating feature, a premium license must be installed on each node in a cluster.

- To locate physical disks or to identify failed physical disks, provision to blink and unblink the physical disks Light Emitting Diodes (LEDs) is provided.
- Support for newer platforms:
  - Platforms based on AX nodes—Dell EMC Solutions for Microsoft Azure Stack HCI nodes: AX-640, AX-6515, and AX-740xd.
  - Platforms based on Storage Spaces Direct Ready Nodes from Dell EMC—Dell EMC Solutions for Microsoft Azure Stack HCI: R440 ,R640,R740xd and R740xd2.
  - Microsoft Windows Admin Center version 1910.2.
- Ability to monitor health and inventory of Accelerators (GPU) with latest iDRAC9 based PowerEdge Servers.
- User interface enhancements for Intel Persistent Memory Health monitoring and Inventory.
- Correlation between Storage Controllers and Physical Disks to view the associated disks.
- Ability to refresh the health, inventory, and iDRAC information of the managed target nodes to ensure that displayed inventory information is the latest.
- Usability enhancement by downloading DSU and IC automatically required for components update.
- Ability to download catalog, DSU, and IC utilities from the Internet using proxy settings to generate compliance report.
- Displays Dell EMC Solutions badge **Azure Stack HCI Certified** for Dell EMC Solutions for Microsoft Azure Stack HCI cluster consisting of AX nodes or Storage Spaces Direct Ready Nodes.

Additional resources

Table 1. Additional resources

Document	Description	Availability
Dell EMC OpenManage Integration with Microsoft Windows Admin Center Installation Guide	Provides information about installing and configuring OpenManage Integration with Microsoft Windows Admin Center.	1. Go to Dell.com/OpenManageManuals. 2. Select **OpenManage Integration with Microsoft Windows Admin Center**. 3. Click **DOCUMENTATION** > **MANUALS AND DOCUMENTS** to access these documents.
Dell EMC OpenManage Integration with Microsoft Windows Admin Center Release Notes	Provides information about new features, known issues and workarounds in OpenManage Integration with Microsoft Windows Admin Center.	
Dell EMC Infrastructure Compliance Report for PowerEdge Servers and Azure Stack HCI Clusters using the OMIMSWAC	This white paper describes the process to generate update compliance report for PowerEdge servers, Microsoft Azure Stack HCI clusters, and Hyper-V based failover clusters by using OMIMSWAC.	
Microsoft Windows Admin Center documentation	For more information about using Microsoft Windows Admin Center.	https://www.microsoft.com/en-us/cloud-platform/windows-admin-center

2

Getting started with OpenManage Integration with Microsoft Windows Admin Center

Before you launch Dell EMC OpenManage Integration extension in Windows Admin Center, ensure that you have:

- Logged in to Windows Admin Center as a gateway administrator.

After installing the OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC), perform the following actions to launch the extension:

1. In the upper left corner of Windows Admin Center, select:
   - For 1910.2 GA release of Windows Admin Center: **Server Manager** or **Cluster Manager** from the drop-down menu.
2. From the list, select a server or cluster connection, and then click **Connect**.
3. Enter the server or cluster credentials.

   NOTE: If you are not prompted to enter the credentials, ensure that you select "Manage as" and enter appropriate Server Administrator or Cluster Administrator accounts.

   NOTE: OMIMSWAC does not support single sign-on and smart card authentication methods.
4. In the left pane of the Microsoft Windows Admin Center, under **EXTENSIONS**, click **Dell EMC OpenManage Integration**.

NOTE: If Microsoft Windows Admin Center is installed on a target node and the target node is managed by OMIMSWAC, the inventory collection functionality of OMIMSWAC may result in failures.

Before connecting to the target node, ensure that you select "Manage as" and provide appropriate Server Administrator or Cluster Administrator accounts. For more information about selecting "Manage as", see the "Get Started with Windows Admin Center" section in the Microsoft documentation.

When you launch the OpenManage Integration for the first time, a customer notice is displayed to indicate the operations performed by the OpenManage Integration such as enabling the USB NIC and creating an iDRAC user on the target node. Click **Accept** to continue to manage the PowerEdge servers by using the OpenManage Integration.

NOTE: After the information from the managed nodes is collected, the previously created iDRAC user is deleted by OMIMSWAC.

To ensure proper functioning of OpenManage Integration with Microsoft Windows Admin Center, ensure that:

- Firewall in your enterprise environment enables communication through SMB port 445.
- Redfish service is enabled on the target node.
- An iDRAC user slot is available on the target node.
- Ensure that the target node is not booted to Lifecycle Controller.
- Target node is not in the reboot state, or is powered off.
- The USB NIC adapter is not disabled on the target node OS.
- The lockdown mode is disabled on target node.
- The PowerShell execution policy is set to RemoteSigned on the system with Windows Admin Center installed and on the target node OS. For more information, see https://www.dell.com/support/article/sln318718/dell-emc-openmanage-integration-with-microsoft-windows-admin-center-omimswac-fails-to-query-host-information.

NOTE: For management of PowerEdge servers, OMIMSWAC uses an internal OS to iDRAC Pass-through interface. By default, iDRAC can be accessed by using the IP address 169.254.0.1/<Subnet> or 169.254.1.1/<Subnet>. However, if the host has another network interface in the same subnet (for example, when tool such as VMFleet is installed), OMIMSWAC might not be able to communicate to the iDRAC from the host OS. To resolve the conflict, log in to iDRAC and change the USB NIC IP address under the OS to iDRAC passthrough section. For more information about assigning this IP address, see the iDRAC documentation on the Dell EMC support site.

To manage:

- PowerEdge servers, see Manage Dell EMC PowerEdge Servers on page 10.

- Microsoft failover clusters created with PowerEdge servers or Azure Stack HCI created with AX nodes or Storage Spaces Direct Ready Nodes from Dell EMC, see Manage Failover Clusters and Azure Stack HCI on page 13.

3

Ports required by Dell EMC OpenManage Integration with Microsoft Windows Admin Center

Table 2. Ports required by Dell EMC OpenManage Integration with Microsoft Windows Admin Center

Functionality of OpenManage Integration with Windows Admin Center	System with Windows Admin Center installed	Target node/ cluster node	System where DRM catalog is available	System where DSU and IC utilities are available	iDRAC of target node/ cluster node
Installation	NA	NA	NA	NA	NA
Uninstallation	NA	NA	NA	NA	NA
Health, Hardware, and iDRAC inventory	445—Outbound	445—Inbound	NA	NA	443 (Default port)
Update tools settings —Test connection	445—Outbound	NA	NA	445—Inbound	NA
Update compliance	NA	445—Inbound	445—Outbound	445—Outbound	NA
Update compliance notifications	445—Outbound	NA	445—Inbound	NA	NA
Target node update and Cluster-Aware update	NA	Default WinRM ports provided by Microsoft	445—Outbound	445—Outbound	443 (Default port)

For more information about the SMB port 445, see https://go.microsoft.com/fwlink/?linkid=2101556.

For more information about WinRM ports, see https://docs.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management.

4

Manage Dell EMC PowerEdge Servers

Prerequisites:

- You must be logged in to Microsoft Windows Admin Center as a Gateway Administrator.
- You must have installed the Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) extension. For more information about the installation procedure, see the *Dell EMC OpenManage Integration with Microsoft Windows Admin Center Installation Guide* at Dell.com/OpenManageManuals.
- Server connections are added in Microsoft Windows Admin Center. For more information about adding server connections, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center.

To manage PowerEdge servers:

1. In the upper left corner of Windows Admin Center, select **Server Manager** from the drop-down menu.
2. From the list, select a server connection, and then click **Connect**.

   NOTE: If you have not entered the server credentials while adding the connection, you must enter the credentials when you are connecting to the server by selecting "Manage as".

3. In the left pane of the Microsoft Windows Admin Center, under **EXTENSIONS**, click **Dell EMC OpenManage Integration**.
4. Select:
   - **Health**—to view the health status of the target node components. A status icon represents the overall health status of the target node. See Health status—Supported target node components on page 11.
   - **Inventory**—to view the detailed hardware inventory information of the target node components. See Hardware inventory—Supported target node components on page 11.
   - **Update**—to view compliance report and to update components to baseline version. See Update PowerEdge servers and nodes of HCI and Failover clusters on page 17.
   - **iDRAC**—to view the iDRAC details of the target node. You can directly launch the iDRAC console from Windows Admin Center by using the OpenManage Integration. See View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters on page 16.

NOTE: The health, hardware inventory, and iDRAC details are cached and will not be loaded each time the extension is loaded. To view the latest health and inventory status and iDRAC details, in the upper-right corner of the Health Status, click Refresh.

NOTE: For modular servers (YX2X, YX3X, YX4X, YX5X, and above models of PowerEdge servers), the following information that is related to fans and power supplies are not displayed:

- **Health status**
- **Attribute values in the hardware inventory table**

NOTE: For YX2X and YX3X models of PowerEdge servers with firmware version earlier than 2.60.60.60, information about the following components are not displayed:

- **Health status—Accelerators, memory, storage controllers, storage enclosures, and physical disks.**
- **Hardware inventory—Accelerators, memory, storage controllers, storage enclosures, physical disks, network devices, and firmware.**

Topics:

Health status—Supported target node components

Health status of the following target node components is displayed:

- CPUs
- Accelerators
- Memory
- Storage Controllers
- Storage Enclosures
- Physical Disks
- iDRAC
- Power Supplies
- Fans
- Voltages
- Temperatures

NOTE: Health status information is available for Accelerators in YX4X models of PowerEdge servers and above with iDRAC version 4.00.00.00 or newer.

NOTE: Intel DIMM memory is identified as IntelPersistent with an icon.

The health statuses are represented by using a doughnut chart. You can select different sections in the doughnut chart to filter the health status of the components. For example, when you select the red section, components with critical health status are only displayed.

To view the latest health status, in the upper-right corner of the **Health** tab, click **Refresh**.

NOTE: For software storage controllers and physical disks that are attached to embedded SATA controller, the health inventory status is displayed as "Unknown".

Hardware inventory—Supported target node components

Hardware inventories of the following target node components are displayed:

- System
- Firmware
- CPUs
- Accelerators
- Memory
- Storage Controllers

  To view the physical disks in a storage controller, under **Related Disks**, click the **View Disks** link. The physical disks are listed in the **Physical Disks** tab.
- Storage Enclosures
- Network Devices
- Physical Disks

  To view the additional properties of a disk, select the disk, and then click **Advanced Properties**. To view the associated storage controller, click the storage controller link under **Advanced Properties**. The associated storage controller is displayed in the **Storage Controllers** tab. If physical disks are attached to the CPU, then the storage controller link will not be available under **Advanced Properties**.

  To blink and unblink the physical disks

  Select a physical disk, click **Blink** to enable the blinking of the LEDs on the physical disk. The LEDs represent the state of physical disks. When the physical disks are blinking, it helps to locate and also to identify the faulty physical disks in your data center. To disable the blinking of the physical disks, select a disk and click **Unblink**.

  NOTE: The blink and unblink operations are not available for:

- **Disks associated to Boot Optimized Storage Subsystem (BOSS) cards.**
- **Devices with iDRAC firmware version less than 3.30.30.30. Update the iDRAC firmware to the latest version to enable blink and unblink operations.**

NOTE:

- **When the blink or unblink operation is running, Refresh button to load the latest health and hardware inventory information is disabled. Also, when the health and hardware inventory is being loaded in OMIMSWAC, blink and unblink operations is disabled.**
- **Blink or unblink operation fails on physical disks that are attached to an embedded SATA controller with an error `Blink/Unblibk May not be supported with - <disk_name>`.**

- Power Supplies
- Fans

To view the latest hardware inventory information, in the upper-right corner of the **Inventory** tab, click **Refresh**.

To view iDRAC details of target node, see View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters on page 16.

NOTE: Under Inventory, the attribute values of a few target node components are displayed as blank because the value might not be available in the target node.

NOTE: Under Firmware inventory, for few network devices with multiple ports, since the applicable firmware version is same for all ports, only a single port with the firmware version will be displayed.

NOTE: Information of few attributes of storage enclosures, firmware inventory, and memory component might not be available for:

- **YX2X and YX3X models of PowerEdge servers.**
- **YX4X models of PowerEdge servers with iDRAC version lesser than 3.30.30.30.**

NOTE: For PCIe SSD Backplane of storage enclosures, few attribute values might not be available.

NOTE: Health status information is available for Accelerators in YX4X models of PowerEdge servers and above with iDRAC version 4.00.00.00 or newer.

NOTE: Intel DIMM memory is identified as IntelPersistent with an icon.

5

Manage Failover Clusters and Azure Stack HCI

Prerequisites:

- You are logged in to Microsoft Windows Admin Center as a Gateway Administrator.
- You must have installed the Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) extension. For more information about the installation procedure, see the *Dell EMC OpenManage Integration with Microsoft Windows Admin Center Installation Guide* at Dell.com/OpenManageManuals.
- You have added failover or hyper-converged cluster connections in Microsoft Windows Admin Center. For more information about adding failover or hyper-converged cluster connections, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center.
- Ensure that all the cluster nodes are reachable using IP address, hostname, or Fully Qualified Domain Name (FQDN) before managing the cluster with OMIMSWAC.

To manage the Microsoft Failover Clusters created with PowerEdge servers and Azure Stack HCI created with AX nodes or Storage Spaces Direct Ready Nodes from Dell EMC:

1. In the upper left corner of Windows Admin Center, select:
   - For 1910.2 GA release of Windows Admin Center: **Cluster Manager** from the drop-down menu.
2. From the list, select a failover or hyper-converged cluster connection, and then click **Connect**.

   NOTE: If you have not entered the failover or hyper-converged cluster credentials while adding the connection, you must enter the credentials when you are connecting to the failover or hyper-converged cluster by selecting "Manage as".

   NOTE: When a cluster is connected by using Single Sign-on authentication, OMIMSWAC is unable to retrieve the inventory information and the Windows Admin Center might be unresponsive. To resolve the issue:

   - **Connect the cluster by using the "Manage as" feature and by entering the cluster administrator account. For more information, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/use/get-started.**
   - **Ensure Windows Admin Center service is running and for more information on troubleshooting Windows Admin Center, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/support/troubleshooting.**
3. In the left pane of the Microsoft Windows Admin Center, under **EXTENSIONS**, click **Dell EMC OpenManage Integration**.
4. To manage a failover or hyper-converged cluster, select:
   - **Health**—to view the health status of the server components of the individual nodes in the cluster.
     - The **Overall Health Status** section displays the overall health of the cluster. Select different sections in the doughnut chart to filter the health status of the components of the cluster nodes.

       NOTE: The overall health status of the cluster might be displayed as critical or warning even though the components of the nodes displayed on the Windows Admin Center are healthy. For more details on the components in critical health state, go to the respective iDRAC console.

     See Health status—Supported target node components in Failover Clusters and Azure Stack HCI on page 14.
   - **Inventory**—to view the detailed hardware inventory information of the component. On the **Overview** page, the basic details of the nodes of the failover or hyper-converged cluster are listed. Select the required node to view detailed hardware inventory of the server components. See Hardware inventory—Supported target node components in Failover Clusters and Azure Stack HCI on page 14.
   - **Update**—to view and update the compliance charts of the nodes and components. Expand the required node to view a detailed compliance report of the components. See Update PowerEdge servers and nodes of HCI and Failover clusters on page 17.
   - **iDRAC**—to view the iDRAC details of the individual nodes. You can directly launch the iDRAC console from Windows Admin Center by using the OpenManage Integration. See View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters on page 16.

NOTE: The health, hardware inventory, and iDRAC details are cached and will not be loaded each time the extension is loaded. To view the latest health and inventory status and iDRAC details, in the upper-right corner of the Health Status, click Refresh.

Topics:

Health status—Supported target node components in Failover Clusters and Azure Stack HCI

On the **Cluster - Azure Stack HCI** page, select the **Health** tab to view the overall health status of the Failover or HCI cluster and the health status of the following target node components of the nodes in Failover Cluster or Azure Stack HCI. Selecting critical or warning section in the overall health status doughnut chart displays corresponding nodes and the components in the critical or warning state respectively.

- CPUs
- Accelerators
- Memory
- Storage Controllers
- Storage Enclosures
- Physical Disks
- iDRAC
- Power Supplies
- Fans
- Voltages
- Temperatures

NOTE: Health status information is available for Accelerators in YX4X models of PowerEdge servers and above with iDRAC version 4.00.00.00 or newer.

NOTE: Intel DIMM memory is identified as IntelPersistent with an icon.

The health statuses are represented by using a doughnut chart. You can select different sections in the doughnut chart to filter the health status of the components. For example, when you select the red section, components with critical health status are only displayed.

In a Failover or HCI cluster, if the different sections of the doughnut chart for individual components are selected, the respective nodes with the component health status are listed. Expand the nodes to view the components in a particular health state.

To view the latest health status, in the upper-right corner of the **Health** tab, click **Refresh**.

NOTE: For software storage controllers and physical disks attached to embedded SATA controller, the health inventory status will always be displayed as "Unknown".

Hardware inventory—Supported target node components in Failover Clusters and Azure Stack HCI

Hardware inventory of the following target node components of the nodes in Failover Cluster or Azure Stack HCI are displayed:

- System
- Firmware
- CPUs
- Accelerators

- Memory
- Storage Controllers

  To view the physical disks in a storage controller, under **Related Disks**, click the **View Disks** link. The physical disks are listed in the **Physical Disks** tab.

  Storage Enclosures
- Network Devices
- Physical Disks

  To view the additional properties of a disk, select the disk, and then click **Advanced Properties**. To view the associated storage controller, click the storage controller link under **Advanced Properties**. The associated storage controller is displayed in the **Storage Controllers** tab. If physical disks are attached to the CPU, then the storage controller link will not be available under **Advanced Properties**.

  To blink and unblink the physical disks

  Select a node and then select a physical disk, click **Blink** to enable the blinking of the LEDs on the physical disk. The LEDs represent the state of physical disks. When the physical disks are blinking, it helps to locate and also to identify the faulty physical disks in your data center. To disable the blinking of the physical disks, select a disk and click **Unblink**. In a cluster, the blink or unblink operation of a selected node must complete before using the blink or unblink operation on a different node.

  NOTE: The blink and unblink operations are not available for:

  - **Disks associated to Boot Optimized Storage Subsystem (BOSS) cards.**
  - **Devices with iDRAC firmware version less than 3.30.30.30. Update the iDRAC firmware to the latest version to enable blink and unblink operations.**
    - **If blink and unblink operation is unavailable for selected supported disks even with iDRAC firmware version 3.30.30.30 and above, then upgrade the iDRAC firmware to the latest version to enable blink and unblink operations.**

  NOTE:

  - **When the blink or unblink operation is running, Refresh button to load the latest health and hardware inventory information is disabled. And, when the health and hardware inventory is loaded in OMIMSWAC, blink and unblink operations is disabled.**
  - **Blink or unblink operation fails on physical disks that are attached to an embedded SATA controller with an error `Blink/Unblibk May not be supported with - <disk_name>`.**
- Power Supplies
- Fans

To view the latest hardware inventory information, in the upper-right corner of the **Inventory** tab, click **Refresh**.

To view iDRAC details of target node, see View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters on page 16.

NOTE: Under Inventory, the attribute values of a few target node components are displayed as blank because the value might not be available in the target node.

NOTE: Under Firmware inventory, for few network devices with multiple ports, since the applicable firmware version is same for all ports, only a single port with the firmware version will be displayed.

NOTE: Information of few attributes of storage enclosures, firmware inventory, and memory component might not be available for:

- **YX2X and YX3X models of PowerEdge servers.**
- **YX4X models of PowerEdge servers with iDRAC version lesser than 3.30.30.30.**

NOTE: For PCIe SSD Backplane of storage enclosures, few attribute values might not be available.

NOTE: Health status information is available for Accelerators in YX4X models of PowerEdge servers and above with iDRAC version 4.00.00.00 or newer.

NOTE: Intel DIMM memory is identified as IntelPersistent with an icon.

6

View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters

To view the following iDRAC details of the target node, select **Server Manager** or **Cluster Manager** from the upper left corner of Microsoft Windows Admin Center, and then select a server or cluster connection from the list. In the left pane, under EXTENSIONS, click **Dell EMC OpenManage Integration** and navigate to the **iDRAC** tab.

NOTE: For failover and hyper-converged clusters, expand the nodes to view the following details.

- **iDRAC IP address. You can launch the iDRAC console directly from Microsoft Windows Admin Center.**
- **IPMI version.**
- **iDRAC firmware version.**

7

Update PowerEdge servers and nodes of HCI and Failover clusters

OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) allows you to generate compliance details and update components, such as BIOS, driver, firmware, and/or system management applications of target nodes and nodes in an HCI and failover clusters. You can use either an online or offline catalog to generate compliance details and update components.

In OMIMSWAC, click **Update**. The update window is displayed.

On this page, you can generate a compliance report and update the components as follows:

1. Generate compliance report: Select update source catalog (online or offline catalog) to fetch the update details for each device and generate a compliance report.
2. Verify compliance report and confirm component selection: Verify the generated compliance report. By default, all the non-compliant components (excluding downgradable component) are selected. Select or clear any components you want to update and then confirm the components selection.
3. Update: Update the target node or cluster.

To generate compliance report and update a target node, see update target node. To generate compliance report and update nodes of HCI and Failover cluster, see update nodes of HCI and failover clusters.

OpenManage Integration uses online or offline catalog to create baselines. The catalog contains latest BIOS, driver, firmware, and/or system management applications. The system management application might include IC, Driver Pack, iSM, OMSA and so on. OpenManage Integration also uses the Dell EMC System Update Utility (DSU) and Dell EMC Inventory Collector (IC) tools to fetch the update details for each device. The DSU and IC tools help to generate compliance report and remediate the non-compliant devices by updating them.

When offline or online catalog is selected, OMIMSWAC collects the DSU and IC tools configured in **Settings** > **Update Tools**. To configure Update Tools, see Configure the update compliance tools setting. If DSU and IC tools are not configured in the Settings, then OMIMSWAC with Internet access will download them from `www.downloads.dell.com`.

In the **Notifications** section of the Windows Admin center, you are notified when a new online or offline catalog file is available. To generate the latest compliance report, on the **Update** tab, run Update Compliance Report.

NOTE: Cluster-Aware Updating (CAU) feature is supported for the following platform with valid licenses:

- **YX4X models of Dell EMC PowerEdge server and above with iDRAC firmware 4.00.00.00 or newer.**
- **Dell EMC Solutions for Microsoft Azure Stack HCI with iDRAC firmware 4.00.00.00 or newer.**

For more information about licenses, see *OpenManage Integration with Windows Admin Center Licensing* in the OMIMSWAC Installation Guide.

Topics:

Configure the update compliance tools setting

To generate the latest update compliance report and device component details, OpenManage Integration without Internet access requires you to configure the settings for the update compliance tools. The supported versions of the Dell System Update (DSU) and Dell Inventory Collector (IC) utilities for OpenManage Integration version 1.1.0 are:

- DSU version: 1.8.1. Download the DSU from https://downloads.dell.com/OMIMSWAC/DSU/.
- IC version: Download the IC from https://downloads.dell.com/OMIMSWAC/IC/.

The following configuration is required when OMIMSWAC is not connected to the Internet and you use Offline-Dell EMC Repository Manager (DRM) catalog to generate compliance report and update the components.

1. In the **Settings** tab, enter the share location where the DSU utility is placed.

DSU is used to apply the Dell update packages to target nodes.

2. Enter the share location where the IC utility is placed.

   The IC utility is used to collect the hardware inventory information from target nodes.

3. Enter the user credentials to access the share location.

   NOTE: When OMIMSWAC is uninstalled, the data present in the Settings page is not deleted. If the OMIMSWAC is later reinstalled, previously configured data in the Settings page is still available to it. However, the password remains unavailable.

4. To confirm if the utilities are accessible, click **Test Connection**.
5. Click **Save** to save the update tools setting.

   The passwords for the update tool settings are retained only for the current browser session. Ensure that you reenter the password after opening a new browser session for the Update compliance feature of OpenManage Integration with Microsoft Windows Admin Center to function properly.

   To generate the latest update compliance report, see Generating compliance report—Target node and Generating compliance report—Target node components in Failover Clusters and Azure Stack HCI.

Configure proxy settings

OMIMSWAC provides an option to download catalog, DSU, and IC utilities from the Internet using proxy settings to generate compliance report. However, OMIMSWAC, which is connected to the Internet by proxy, does not support updating target nodes or clusters using online catalogs. In this case, compliance and updates using the offline catalog are supported.

You can configure the proxy settings to connect to a proxy server that acts as an intermediary between your gateway system and the Internet. If OMIMSWAC update compliance tool settings are not configured and the gateway system is not connected to the Internet, it will check the Internet connectivity using the proxy settings.

To connect to a proxy server:

1. Enter the IP address of the proxy server in the below format:

   `https://<IP address>` or **`http://<IP address>`**

2. Enter the Port number of the proxy server in the below format, and click **Save**.

   `<port number> (https)` or **`<port number> (http)`**

   For example: 443 (https) or 80 (http)

   To generate the latest update compliance report, see Generating compliance report—Target node and Generating compliance report—Target node components in Failover Clusters and Azure Stack HCI.

Update target nodes

By using OpenManage Integration with Windows Admin Center, you can view the compliance report (BIOS, driver, firmware, and/or system management application) and update the components of target nodes.

Compliance and update prerequisites

Before you generate a compliance report and update components, ensure the following:

- Software and hardware requirements listed in the *compatibility matrix* of the *Installation Guide* are met.
- To manage a target node, connect to the target node using **Manage as** option and provide appropriate target node administrator credentials. And ensure that the user is part of the local user group of gateway administrators. For more information about selecting "Manage as", see the "Get Started with Windows Admin Center" section in the Microsoft documentation.
- Take care of the workload before updating the target node.
- Ensure that inventory information for the target node has been retrieved.
- Ensure that iDRAC lockdown mode is disabled. To disable iDRAC system lockdown mode, see iDRAC documents.
- For SAS-RAID_Driver, ensure the followings:
  - Set the SATA controller to RAID mode.
  - Set the NVMe PCIe SSDs to RAID mode.

  For more information about setting the RAID mode, see Appendix
- Ensure that the WAC is not installed on the target node you want to update.
- Ensure that the target node is reachable using IP address, hostname, and Fully Qualified Domain Name (FQDN) of the target node.

NOTE: If the target node is not reachable, and the target node update is performed, the update status may show failed. In this case, if you reboot the target node immediately after update and rerun the compliance, the target node components status may show compliant, whereas the overall target node update status may still show failed.

NOTE: Updating a target node where WAC is installed is not recommended. To support this scenario, install the WAC on another target node (non WAC related) and complete the update.

NOTE: While the compliance or update is in progress, it is not allowed to run any further compliance or update task for the same target node that includes the update requests from the MS WAC Update tools.

Step 1: Generating compliance report—Target node components

To generate a compliance report for a target node, select **Update > Update Source**, and choose any of the available offline or online catalog options as follows:

Generating compliance report using online catalog

To use online catalog, OMIMSWAC must be connected to the Internet with or without proxy settings. OMIMSWAC with Internet access allows you to use the online catalog option in the **Update Source** drop-down list to automatically download the catalog.

To view the compliance details, perform the following action:

1. Under **Update > Update Source**, choose any of the available online catalog options.

   The corresponding online catalog is selected by default based on the target node.

   Available online catalogs vary depending on the target node/cluster you are connected to as follows:

   - For PowerEdge servers: Dell EMC Enterprise Catalog which contains the validated versions of components for PowerEdge servers.
   - For MX servers: Dell EMC MX Solution Catalog which contains the validated versions of components for PowerEdge MX Modular.
   - For Azure Stack HCI Cluster nodes: Dell EMC Azure Stack HCI Solution Catalog which contains the validated versions of components for AX nodes and Storage Spaces Direct Ready Nodes.
2. Select **Next: Compliance details:** to generate compliance report.

OMIMSWAC downloads the catalog, collects the DSU and IC tools that are configured in the **Settings** tab, and generates a Compliance Report. If DSU and IC tools are not configured in the **Settings**, then OMIMSWAC downloads them from `www.downloads.dell.com` to generate the compliance report.

The compliance details are computed and the report is available under **Update** > **Compliance Details**. For more details about compliance report, see View compliance report.

Generating compliance report using offline catalog

OMIMSWAC with or without Internet access allows you to select the Offline - Dell EMC Repository Manager Catalog to generate compliance report.

Before you generate the latest compliance report of target node components, ensure the followings. The following prerequisites are required when OMIMSWAC is not connected to the Internet and the Offline-Dell EMC Repository Manager (DRM) catalog is used to generate a compliance report and update components.

- Configure the share location details where the DSU and IC applications are placed. See Configure the update compliance tools setting.
- Generate the latest catalog files by using the Dell EMC Repository Manager (DRM) application. The supported version of DRM can be downloaded from Dell EMC Repository Manager.

To view the compliance details, perform the following actions:

1. Under **Update** > **Update Source**, choose **Offline - Dell EMC Repository Manager Catalog** from the drop-down list. By default, online catalog is selected.

   Offline - Dell EMC Repository Manager Catalog: When the DRM repositories are available in a shared location and is applicable for all managed nodes by OMIMSWAC in data centers with no Internet connectivity.
2. Enter the CIFS share path where catalog files are placed and the user credentials to access the CIFS share path, and then select **Next: Compliance details:**.

The catalog files can be generated by using the Dell EMC Repository Manager (DRM) application. Ensure that in the shared catalog repository all the required Dell Update Packages (DUP) are available for the target node.

If a new catalog path is provided, the previous path that was used to compute the update compliance may not be available.

OMIMSWAC collects the catalog from the shared path, collects the DSU and IC tools that are configured in the **Settings** tab, and generates a Compliance Report. If DSU and IC tools are not configured in the **Settings**, OMIMSWAC with Internet access will download them from `www.downloads.dell.com` to generate the compliance report.

NOTE: You must provide individual catalog files with the user credentials for server manager, and cluster manager respectively.

The compliance details are computed and the report is available under **Update** > **Compliance Details**. For more details about compliance report, see View compliance report.

Step 2: Viewing compliance report and selecting components—Target node components

The update compliance details are computed, and the compliance report is displayed. The doughnut chart represents the number of components in compliant, urgent, recommended, and optional states using color codes. The compliance report provides a detailed view of all the components that contains: component name, current version, type, baseline version, compliance status, criticality, and Compliance Type.

Attribute names	Description
Component Name	Specifies component name. For example: `Serial-ATA_Firmware_6FGD4_WN64_E012_A00`
Compliance	Specifies compliance type whether compliant or non-compliant. • `Compliant` - Target nodes in this category have the same versions of BIOS, drivers, firmware, and system management application as that of the imported catalog. • `Non-Compliant` - Target nodes in this category require BIOS, drivers, firmware, or system management application updates.
Criticality	Specifies whether compliance is urgent, recommended, or optional. • `Urgent` - The update contains changes to improve the reliability and availability of the Dell EMC system or related component. Therefore, apply this update immediately. • `Recommended` - The update contains feature enhancements or changes that help keep the system software current and compatible with other system modules (firmware, BIOS, drivers, and system management application). • `Optional` - The update contains changes that impact only certain configurations, or provides new features that may/may not apply to the environment. Review the update specifications to determine if it applies to the system.
Current Version	Specifies the current component version. For example: `E012`
Baseline Version	Specifies the version belongs to the imported catalog. For example: `E013`
Type	Specifies the component type. For example: `Firmware`, `BIOS`, `Driver`, `Application`
Compliance Type	Specifies whether the component is Upgradable, Downgradable, or Same.

	• `Upgradable`: Component can be upgraded from the current version. • `Downgradable`: Component can be downgraded from the current version. • `Same`: Component current verison is same as the baseline version.

1. By default, all the non-compliant upgradable components are selected.

   Clear the selected components or select the non-compliant downgradable components that you want to update. However, if you want to change any of the default selections, ensure that the dependencies between the corresponding component firmware and drivers are met.
2. Once components are selected for update, under **Compliance Details**, click **Next: Summary** to proceed to the summary report page for confirmation.

   NOTE: When components are selected and confirmed, if lockdown mode is enabled in iDRAC on the target node, an error occurs and you cannot proceed to update. Disable the lockdown mode on the target node that is being managed by OMIMSWAC before updating the target node. To disable iDRAC system lockdown mode, see iDRAC documents.

   - To change the components selection during update operation, in the **Summary** tab, click **Back** to go to the **Compliance Details** tab, and select or clear the selection of components.
   - If you want to change the update source and rerun the compliance, click **Exit** to go to the **Update Source**.

NOTE: If a catalog does not contain updates to a component, then the component is not displayed in the compliance report generated by using OpenManage Integration with Microsoft Windows Admin Center integration.

Step 3: Updating—Target node components

After generating the compliance report in the **Compliance Details** tab and confirming the components selection in the **Summary** tab, you can proceed to update the target node components as follows:

1. To update the BIOS, driver, firmware, and/or system management application of the PowerEdge server to the latest version, under **Summary**, click **Next: Update**. You will be directed to the **Update Status** window.

   NOTE: While the update is in progress, it is not recommended to exit or close the browser. If you close or exit the browser, target node update may fail.
2. OMIMSWAC notifies once the update job is finished.

   - After successful update, compliance report (based on the previous selections) will be recomputed automatically and displayed in the **Update** tab.
   - If the update operation fails, check the log files stored at the following path for more details.
     - Gateway system: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp \generated\logs`
     - Windows 10 gateway system: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp \generated\logs`
   - To run the compliance report again, click **Re-run Compliance** and provide the compliance settings details.

Update nodes of HCI and failover clusters

The Cluster-Aware Updating (CAU) feature in OpenManage Integration with Windows Admin Center (OMIMSWAC) allows you to view the compliance report (BIOS, driver, firmware, and/or system management application) and update the components of nodes of HCI and failover clusters without affecting the workloads.

NOTE: The CAU feature is supported for the following platforms with valid licenses:

- **YX4X models of Dell EMC PowerEdge server and above with iDRAC firmware 4.00.00.00 or newer.**
- **Dell EMC Solutions for Microsoft Azure Stack HCI with iDRAC firmware 4.00.00.00 or newer.**

Compliance and update prerequisites

Before you generate a compliance report and update components, ensure the following:

- Software and hardware requirements listed in the *compatibility matrix* of the *Installation Guide* are met.

- Ensure that the cluster service is up before running the update compliance. When the cluster service is down, an update compliance report for a target node may not be generated.
- To manage a cluster, connect to the cluster using **Manage as** option and provide appropriate cluster administrator credentials. And ensure that the user is part of the local user group of gateway administrators. For more information about selecting "Manage as", see the "Get Started with Windows Admin Center" section in the Microsoft documentation.
- Ensure that inventory information for the target node has been retrieved.
- Ensure both physical, and virtual disks are in healthy state before triggering CAU.
- Ensure that iDRAC lockdown mode is disabled. To disable iDRAC system lockdown mode, see iDRAC documents.
- For SAS-RAID_Driver, ensure the followings:
  - Set the SATA controller to RAID mode.
  - Set the NVMe PCIe SSDs to RAID mode.

  For more information about setting the RAID mode, see Appendix
- Ensure that the target node is reachable using IP address, hostname, and Fully Qualified Domain Name (FQDN) of the target node.

  NOTE: If the target node is not reachable, and the target node update is performed, the update status may show failed. In this case, if you reboot the target node immediately after update and rerun the compliance, the target node components status may show compliant, whereas the overall server update status may still show failed.
- Ensure that OMIMSWAC premium licenses are installed on all cluster nodes to use the CAU feature. To verify the licensing, you can generate a compliance report to view the license installed on each node.

NOTE: It is recommended to validate the cluster before triggering CAU. For more information about validating a cluster, see Microsoft documents Validate Hardware for a cluster.

NOTE: Updating a cluster where WAC is installed on a cluster node is not recommended. To support this scenario, install the WAC on another system that is not part of the cluster and complete the update.

NOTE: While the compliance or update is in progress, it is not allowed to run any further compliance or update task for the same cluster that includes the update requests from the MS WAC Update tools.

NOTE: The CAU feature is not supported for YX2X and YX3X models of Dell EMC PowerEdge servers.

Step 1: Generating compliance report—Target node components in Failover Clusters and Azure Stack HCI

To generate a compliance report for target node components in Failover Clusters and Azure Stack HCI, select **Update > Update Source**, and choose any of the available offline or online catalog options as follows:

Generating compliance report using online catalog

To use online catalog, OMIMSWAC must be connected to the Internet. OMIMSWAC with Internet access allows you to use the online catalog option in the **Update Source** drop-down list to automatically download the catalog.

To view the compliance details, perform the following action:

1. Under **Update > Update Source**, choose any of the available online catalog options. The corresponding online catalog is selected by default based on the cluster.

   Available online catalogs vary depending on the cluster/target node you are connected to as follows:

   - For PowerEdge servers: Dell EMC Enterprise Catalog which contains the validated versions of components for PowerEdge servers.
   - For MX servers: Dell EMC MX Solution Catalog which contains the validated versions of components for PowerEdge MX Modular.
   - For Azure Stack HCI Cluster nodes: Dell EMC Azure Stack HCI Solution Catalog which contains the validated versions of components for AX nodes and Storage Spaces Direct Ready Nodes.
2. Select **Next: Compliance details:** to generate compliance report.

OMIMSWAC downloads the catalog, collects the DSU and IC tools that are configured in the **Settings** tab, and generates a Compliance Report. If DSU and IC tools are not configured in the **Settings**, then OMIMSWAC downloads them from `www.downloads.dell.com` to generate the compliance report.

You will be directed to the compliance report generated in the **Compliance Details** window. For more details about compliance report, see View compliance report.

Generating compliance report using offline catalog

OMIMSWAC with or without Internet access allows you to select the Offline - Dell EMC Repository Manager Catalog to generate compliance report.

Before you generate the latest compliance report of a cluster, ensure the followings. The following prerequisites are required when OMIMSWAC is not connected to the Internet and the Offline-Dell EMC Repository Manager (DRM) catalog is used to generate a compliance report and update components.

- Configure the share location details where the DSU and IC applications are placed. See Configure the update compliance tools setting.
- Generate the latest catalog files by using the Dell EMC Repository Manager (DRM) application. The supported version of DRM can be downloaded from Dell EMC Repository Manager.

To view the compliance details, perform the following actions:

1. Under **Update** > **Update Source**, choose **Offline - Dell EMC Repository Manager Catalog** from the drop-down list. By default, online catalog is selected.

   Offline - Dell EMC Repository Manager Catalog: When the DRM repositories are available in a shared location and is applicable for all managed devices by OMIMSWAC in data centers with no Internet connectivity.

   NOTE: It is recommended that the Azure Stack HCI catalog files be used to generate a compliance report for Azure Stack HCI.
2. Enter the CIFS share path where catalog files are placed and the user credentials to access the CIFS share path, and then select **Next: Compliance details:** to generate compliance report.

   The catalog files can be generated by using the Dell EMC Repository Manager (DRM) application. Ensure that in the shared catalog repository all the required Dell Update Packages (DUP) are available for the target node.

   If a new catalog path is provided, the previous path that was used to compute the update compliance may not be available.

OMIMSWAC collects the catalog from the shared path, collects the DSU and IC tools that are configured in the **Settings** tab, and generates a Compliance Report. If DSU and IC tools are not configured in the **Settings**, OMIMSWAC with Internet access will download them from `www.downloads.dell.com` to generate the compliance report.

NOTE: You must provide individual catalog files with the user credentials for server manager, and cluster manager respectively.

You will be directed to the compliance report generated in the **Compliance Details** window. For more details about compliance report, see View compliance report.

Step 2: Viewing compliance report and selecting components—Target node components in Failover Clusters and Azure Stack HCI

The update compliance details are computed, and the compliance report is displayed. The doughnut chart represents the number of components in compliant, urgent, recommended, and optional states using color codes. The Compliance Report provides a detailed view of all the components that contains component name, current version, type, baseline version, compliance status, criticality, and Compliance Type.

For HCI and failover clusters, the update compliance of the individual target nodes and the components are represented by using two doughnut charts—Node Summary and Component Summary. To analyze further, check the individual nodes in the Compliance Report to get the current version, baseline versions and compliance type of the components, and to view all the nodes and components in non-compliant, urgent, recommended, and optional states respectively.

Along with compliance information, the license status (OMIMSWAC premium license) for each node is also displayed. All target nodes participating in the cluster must have valid licenses, otherwise, you cannot proceed to update the cluster. For more information about OMIMSWAC licensing, refer to OMIMSWAC Installation Guide.

Attribute names	Description
Component Name	Specifies component name. For example: `Serial-ATA_Firmware_6FGD4_WN64_E012_A00`
Compliance	Specifies compliance type whether compliant or non-compliant.

	• `Compliant` - Target nodes in this category have the same versions of BIOS, drivers, firmware, and system management application as that of the imported catalog. • `Non-Compliant` - Target nodes in this category require BIOS, drivers, firmware, or system management application updates.
Criticality	Specifies whether compliance is urgent, recommended, or optional. • `Urgent` - The update contains changes to improve the reliability and availability of the Dell EMC system or related component. Therefore, apply this update immediately. • `Recommended` - The update contains feature enhancements or changes that help keep the system software current and compatible with other system modules (BIOS, driver, firmware, and system management application). • `Optional` - The update contains changes that impact only certain configurations, or provides new features that may/may not apply to the environment. Review the update specifications to determine if it applies to the system.
Current Version	Specifies the current component version. For example: `E012`
Baseline Version	Specifies the version belongs to the imported catalog. For example: `E013`
Type	Specifies the component type. For example: `Firmware`, `BIOS`, `Driver`, `Application`
Compliance Type	Specifies whether the component is Upgradable, Downgradable, or Same. • `Upgradable`: Component can be upgraded from the current version. • `Downgradable`: Component can be downgraded from the current version. • `Same`: Component current verison is same as the baseline version.

1. By default, all the non-compliant upgradable components are selected for update.

   Clear the selected components or select the non-compliant downgradable components that you want to update. However, if you want to change any of the default selections, ensure that the dependencies between the corresponding component firmware and drivers are met.
2. Once components are selected, under **Compliance Details**, click **Next: Summary** to proceed to the summary report page for confirmation.

   NOTE: When components are selected and confirmed, if lockdown mode is enabled in iDRAC on a target node, an error occurs and you cannot proceed to update. Disable the lockdown mode on the target node that is being managed by OMIMSWAC before updating the cluster. To disable iDRAC system lockdown mode, see iDRAC documents.

   - To change the components selection during update operation, in the **Summary** tab, click **Back** to go to the **Compliance Details** tab, and select or clear the selection of components.
   - If you want to change the update source and rerun the compliance, click **Exit** to go to the **Update Source**.

NOTE: If a catalog does not contain updates to a component, then the component is not displayed in the compliance report generated by using OpenManage Integration with Microsoft Windows Admin Center integration.

Step 3: Updating—Target node components in Failover Clusters and Azure Stack HCI

After generating the compliance report in the **Compliance Details** tab and confirming the components selection in the **Summary** tab, proceed to update the target node components in Failover Clusters and Azure Stack HCI as follows:

1. To update the BIOS, driver, firmware, and/or system management application of target node components in Azure Stack HCI and Failover cluster to the latest version, under **Summary**, click **Next: Cluster Aware Update**.

   A message is prompted to enable CredSSP.
2. Click **Yes** to enable the CredSSP and continue updating the selected components. You will be directed to the **Update Status** window.

   To improve security, disable the CredSSP after the update operation is complete.

   NOTE: While the update is in progress in the Update Status window, it is not recommended to exit or close the browser. If you close or exit the browser, cluster update may fail.

   The update job continues in the background regardless of whether the UI session is alive or not. If the UI session is alive, node level progress status is displayed. OMIMSWAC notifies once the update job is finished.

   - After successful update, compliance report (based on the previous selections) will be recomputed automatically and displayed in the **Update** tab.
   - If the update operation fails, check the log files stored at the following path for troubleshooting purposes.
     - Gateway system: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs`
     - Windows 10 gateway system: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs`
   - To run the compliance report again, click **Re-run Compliance** and provide the compliance settings details.

NOTE: If an update job fails, the updated components will not be rolled back to the old version. Due to this, sometimes the BIOS, firmware, or driver version across nodes in the cluster will not be at the same level. In this case, rerun the update by excluding the updated component.

8

Troubleshooting

Topics:

Availability of OMIMSWAC extension logs

The OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) extension logs of target nodes and cluster nodes are available at `<Windows Directory>\Temp\OMIMSWAC` on target nodes. The logs capture information when the OMIMSWAC functionalities are run and also provide debug information about any errors that occur while performing any OMIMSWAC operations. The logs of various OMIMSWAC functionalities can be easily accessed with the help of the following naming convention:

- For hardware and health inventory: `Inventory<ID*>`
- For update compliance: `FirmwareCompliance<ID*>`
- For update notifications: `Notification<ID*>`

Availability of update operation logs

The application logs for the update compliance feature is available at the following path:

- Gateway system: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated \logs`
- Windows 10 gateway system: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated \logs`

Online catalogs download status is captured in the application logs and can be referred to troubleshoot any download errors in the online catalogs.

When online catalog source is selected, and if DSU and IC are not configured in settings in advance, OMIMSWAC will download the catalog, DSU, and IC utilities in the following path:

- Gateway system: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated \Share\temp\<server/cluster_name>`
- Windows 10 gateway system: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated \Share\temp\<server/cluster_name>`

Ensure that the downloaded catalog file, DSU and IC are not modified during compliance generation and update. The catalog file, DSU, and IC utilities are automatically removed after the compliance report is generated and updated.

Logs for pre update script running on HCI clusters to put storage into maintenance mode are available at `<Windows Directory> \Temp\precau.log` on each node. And logs for post update script running on HCI clusters to restore storage from maintenance mode are available at `<Windows Directory>\Temp\postcau.log` on each node.

Unable to copy the required files to the target node to fetch inventory information.

Ensure that:

- Target node is not in the reboot state and is powered on.
- Firewall is not blocking communication through SMB port 445. For more information, see prepare your environment for Windows Admin Center.
- The user is logged in with Gateway Administrative privileges. Before connecting to the target node, ensure that you select "Manage as" and provide appropriate Server Administrator or Cluster Administrator accounts. For more information about selecting "Manage as", see the "Get Started with Windows Admin Center" section in the Microsoft documentation.

Unable to fetch the health and hardware inventory from iDRAC.

To fetch the health and hardware inventory information from iDRAC, ensure that:

- For management of PowerEdge servers, OMIMSWAC uses an internal operating system to iDRAC Pass-through interface. By default, iDRAC is reachable using the IP address 169.254.0.1/<*Subnet*> or 169.254.1.1/<*Subnet*>. However, if the host has another network interface in the same subnet (for example, when tool such as VMFleet is installed), OMIMSWAC might not be able to communicate to the iDRAC from the host operating system.

  To resolve the conflict, log in to iDRAC and change the USB NIC IP address under the operating system to iDRAC passthrough section. For more information about assigning this IP address, see the iDRAC documentation on the support site.
- For management of Clusters, all the cluster nodes are reachable using IP address, Hostname, and Fully Qualified Domain Name (FQDN) before managing the cluster with OMIMSWAC.
- If the Redfish service is disabled, enable the Redfish service by using iDRAC UI. For more information, see the iDRAC documentation on Dell EMC support site.
- User slots are available on iDRAC to create new users.

Unable to complete or select the disks for the blink or unblink operations.

- **Cause**: The Redfish service is not enabled.

  Resolution: Enable the Redfish service by using iDRAC UI. For more information, see the iDRAC documentation on Dell EMC support site.
- **Cause**: After the hardware inventory is loaded in OMIMSWAC, if the physical disk is removed then the blink and unblink operations fail with error: `Blink may not be supported with <Disk_Name>`.

  Resolution: Insert the physical disk and click **Refresh** to reload the inventory information in OMIMSWAC, and rerun the blink and unblink operations.
- **Cause**: If the iDRAC firmware version is less than 3.30.30.30, the physical disks cannot be selected to blink or unblink.

  Resolution: Update the iDRAC firmware to the latest version and retry the blink and unblink operations.
- Blink and unblink operations fail when a physical disk is attached to an embedded SATA controller and the health status is `Unknown`, indicating that blink or unblink operation may not be supported on the disk.

Licensing status is Unknown or Non-licensed

If the license status is `Unknown` or `Non-licensed`, ensure that:

- License is not expired.
- Licenses are present on each target node.
- Target node is not in the reboot state and is powered on.
- Redfish is enabled.
- Azure stack HCI license or PowerEdge server license is imported onto the respective hardware. Importing Azure stack HCI license to a PowerEdge server or PowerEdge server license to a Azure stack HCI server is not supported.

If the problem persists:

1. Go to iDRAC.
2. Ensure that Redfish service is enabled.
3. Disable OS to iDRAC Pass-through and then enable it.

   For more information about enabling or disabling OS to iDRAC Pass-through, see iDRAC user guide.

Availability of licensing logs

The license related logs are available at the following path and can be found by searching *DellLicenseCollection* in the *Cleanup* file.

- Gateway system: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated \logs\CleanupXXXXXXXXXXXXXX.log`
- Windows 10 gateway system: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated \logs\CleanupXXXXXXXXXXXXXX.log`

Job failed while downloading the required components for the server and cluster-aware updating operations.

Cause: While exporting the repository by using Dell EMC Repository Manager (DRM), the export job may complete with status as "Partially succeeded." In this case, one or many DUPs may be missing from the repository.

Resolution: Retry exporting the repository in DRM and ensure that the job is successfully completed.

Cause: One or many components may not be downloaded when the update source is selected as an online source.

Resolution: Ensure that there is Internet connectivity and retry downloading the catalog from the online source. For more information, see Dell EMC Repository Manager user guide.

CredSSP failed during update

- **Cause**: While updating a cluster, credential delegation using CredSSP may fail.

  Resolution: Reconnect the cluster using fully qualified domain name, and click **Use this credential for all servers** check box.

  For example, if the domain name is test.dev.com, use **`test.dev.com\administrator`** as the domain name, and then click **Use this credential for all servers** check box.
- **Cause**: When using CredSSP authentication to run scripts on a remote machine, the update job may fail with an error.

  The issue is because CredSSP has been disabled in the gateway machine.

  Resolution: To resolve the issue, follow the steps below:

  1. From PowerShell window, run `gpedit`
  2. In the Group Policy Editor window, **Computer Configurations** > **Administrative Templates** > **System** > **Credentials Delegation**
  3. Select **Allow delegating fresh credentials with NTLM-only server authentication** and enable it.
  4. Execute `gpupdate /force` in the PowerShell.

Enabling CredSSP delegation

Cause: When you navigate out of OpenManage Integration to other tools under HCI or Failover solutions and navigate back to OpenManage Integration, the following error is displayed: `Enabling CredSSP Delegation`.

Resolution: Ignore the error because the functionality of OpenManage Integration and Windows Admin Center is not blocked.

Job failed while generating compliance report

Cause: When generating a compliance report, the compliance report generation may fail with the following error in the log:

```
Starting a command on the remote server failed with the following error message : The WinRM client sent a request to the remote WS-Management service and was notified that the request
```

`size exceeded the configured MaxEnvelopeSize quota. For more information, see the about_Remote_Troubleshooting Help topic.`

Resolution: Ensure that:

- Network connectivity between the gateway system and the target node is intact.
- File copying works between the gateway system and the target node. To check this:
  1. Create a session based on target node credential by executing the following PowerShell command:

     ```
     $SecurePassword = convertto-securestring <password> -asplaintext -force

     $credential = New-Object System.Management.Automation.PSCredential -ArgumentList <userid>, $SecurePassword

     $session = New-PSSession -ComputerName <MN FQDN> -Credential $credential -ErrorAction SilentlyContinue
     ```

  2. Copy a test file to the failed target node assuming "Test.txt" is in C:\ drive

     ```
     Copy-Item -Path "C:\Test.txt" -Destination "C:\" -Recurse -Force -ToSession $session
     ```

- If the problem persists after performing the above actions, try restarting the Windows Remote Management (WS-Management) service in the target node (file copy is failing) then re-run the compliance.

Cause: When generating a compliance report for a cluster, the compliance report generation may fail for cluster nodes.

Resolution: Ensure that:

- The cluster service is running on the cluster node by using the `Get-ClusterService` PowerShell command.
- The cluster node is not rebooting or in the powered-off state.

Cause: When generating a compliance report using Windows 10 Microsoft Edge browser, the compliance report generation may fail with the following error: `Unable to generate compliance report. The Manage As credentials have not been set or are not in domain\user format.`

Resolution: Do any of the followings:

- Connect the target node with credentials using Fully Qualified Domain Name (For example, **`domain.lab\username`**) or Top Level Domain (For example, **`domain\username`**).
- Clear the cache memory of the browser and rerun the compliance.
- Ensure the DNS is configured properly in the WAC installed system to connect to the target node with right credentials.

Cause: When you connect to a server or cluster using a password that contains any of the following special characters, and attempt to generate a compliance report using OMIMSWAC, the compliance generation may fail. The special characters are: double-quote ("), grave accent (`), and semi-colon (;).

Resolution: Reset the password by removing special characters and reconnect to the server or cluster.

Job failed while updating the selected components.

Sometimes, CAU or target node update may fail. The causes and resolutions are given below:

- In case of CAU, validate the cluster before triggering Cluster-Aware Updating. For more information about validating a cluster, see Microsoft document Validate Hardware for a cluster.
- **Cause**: Compliance Inventory file is not available for some nodes or file copying from node to gateway is failed after compliance generation.

  Resolution: Rerun the compliance.
- **Cause**: Due to Internet connectivity issue, the followings may fail:
  - Signature verification of DSU or IC
  - Downloading of online catalog
  - Downloading of DUP

  If any of the above fails, CAU or server update also fails.

  Resolution: Ensure that there is Internet connectivity and rerun compliance and update.
- **Cause**: DSU installer is not cleared from a node because the installer file sometimes gets locked by the Windows Admin Center process (sme.exe).

  Resolution: Restart the Windows Admin Center service from Windows Services consoles.

- **Cause**: CAU fails if any of the disks is not in healthy state.

  Resolution: Ensure both physical and virtual disks are in healthy state before triggering CAU. If any disk is in an unhealthy healthy state, refer to the Microsoft document to get it to a healthy state.
- **Cause**: CAU fails if any of the cluster nodes is paused.

  Resolution: Resume cluster nodes (Failover roles) before triggering CAU.

Component showing non-compliant after update

After update, you may see components showing as non-compliant.

Resolution: In this case, check the cleanup logs having the DSU logs to see if there is any ERROR for the component. If there is any prerequisite that is required for the component before update, follow the prerequisite and then rerun the update.

OpenManage Integration access denied

Cause: When you log in to Windows Admin Center (WAC) using gateway user credentials without admin privileges and try to launch OpenManage Integration from the WAC console, access denied error may appear.

Resolution: Before you launch Dell EMC OpenManage Integration extension in Windows Admin Center, ensure to log in to WAC as a gateway administrator.

Dell Update Package failures

The Dell EMC Update Package (DUP) may fail to update components after you trigger an update. There are various reasons for the DUP to fail during the update. Look at the following possible solutions to resolve the issue:

- In Windows Admin Center (WAC) installed machine, check the log files to get more information regarding DUP download failure and component mapping. The component mapping is provided to identify the component (selected for update) in the DUP catalog. The log files are at the following path.

  Gateway system:

  - Server update: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\<PrepareUpdate XXXX>`
  - CAU: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\Update XXXX`

  Windows 10 gateway system:

  - Server update: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\<PrepareUpdate XXXX>`
  - CAU: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\Update XXXX`
- Sample log messages are given below:
  - DUP download failure error log

    ```
    28-Apr-2020 12:19:18 AM::: Error >>> Message : DUPs for some of the selected components are not present in DRM repository.
    ```
  - Component mapping log file

    ```
    ## Format: :>> Component Name -> Package Name

    :>> [0001] Broadcom NetXtreme Gigabit Ethernet ->
    Network_Firmware_RG25N_WN64_21.60.2_01.EXE
    ```
- In the target node, refer component mapping and find the component related DUP log file and check the return code specified in `<Windows Directory>\Dell\UpdatePackage\log\<Package Name>`. See Dell EMC Update Package user guide for cause and possible resolution.

  A return code sample of a DUP failure scenario is given below:

  ```
  Exit code = 1 (Failure)

  2020-04-21 23:48:27

  Update Package finished. Exit code = 1
  ```

- The DUP may fail when attempting to downgrade a driver component to a lower version. In this case, uninstall the driver from the operating system then rerun the component update from OMIMSWAC. For more information about how to uninstall drivers, see Microsoft document.

Alternatively, you can also try the followings:

- Reset and update the iDRAC to version 4.20.20.20 or higher and then rerun the update. For more information about how to Reset or update iDRAC, see iDRAC documentation.
- Run the update manually in the target node by downloading from the path specified in `<Windows Directory>\Dell \UpdatePackage\log\<Package Name>` in the DUP log. Example for a network firmware is https://downloads.dell.com/FOLDER06091050M/1/Network_Firmware_TWFF6_WN64_16.26.60.00.EXE.
- Ensure that the selected DUP is supported on the selected operating system and platform by searching the component name in the Dell Support site. Dell support site URL: https://www.dell.com/support/home/in/en/inbsd1/?app=products.

Test-Cluster fails with network communication errors

Cause: With USB NIC enabled in iDRAC, if you run Test-Cluster command to verify the cluster creation readiness or cluster health, you may see an error in the validation report. The error states that the IPv4 addresses assigned to the host operating system USB NIC cannot be used to communicate with the other cluster networks. This error can be safely ignored.

Resolution: Disable the USB NIC (labeled as Ethernet by default) temporarily before running the Test-Cluster command.

USB NIC network shows as partitioned cluster network

Cause: When the USB NIC is enabled in iDRAC, cluster networks in the failover cluster manager show the networks that are associated with the USB NIC as partitioned. This issue occurs since the cluster communication is enabled by default on all network adapters and USB NIC IPv4 addresses cannot be used to communicate externally, therefore, breaking cluster communication on those NICs. This error can be safely ignored.

Resolution: Disable cluster communication with the networks associated with the USB NICs from the cluster manager.

9

Identifying the generation of your Dell EMC PowerEdge server

To cover a range of server models, the PowerEdge servers are now be referred to using the generic naming convention and not their generation.

This topic explains how to identify the generation of a PowerEdge server that are referred to using the generic naming convention.

Example:

The R740 server model is a rack, two processor system from the 14th generation of servers with Intel processors. In the documentation, to refer to R740, generic naming convention **YX4X** server is used, where:

- The letter **Y** (alphabet) denotes the type (form factor: Cloud (C), Flexible(F), Modular (M or MX), Rack(R), Tower(T)) of the server.
- The letter **X** (digit) denotes the class (number of processors) of the server.
- The digit **4** denotes the generation of the server.
- The letter **X** (digit) denotes the make of the processor.

Table 3. PowerEdge servers naming convention and examples

YX5X servers	YX4X servers	YX3X servers
PowerEdge R7515	PowerEdge M640	PowerEdge M630
PowerEdge R6515	PowerEdge R440	PowerEdge M830
	PowerEdge R540	PowerEdge T130

10

Contacting Dell EMC

Dell EMC provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area.

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell EMC product catalog.

To contact Dell EMC for sales, technical support, or customer service issues:

1. Go to Dell.com/support.
2. Select preferred country or region from the list at the bottom right of the page.
3. Click **Contact Us** and select the appropriate support link.

A

Glossary

The following table defines or identifies abbreviations and acronyms used in this document.

Table 4. Glossary

Abbreviations/ Acronyms	Definition
OMIMSWAC—OpenManage Integration with Microsoft Windows Admin Center	Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) enables IT administrators to manage the PowerEdge servers as hosts, Microsoft Failover Clusters created with PowerEdge servers, and Hyper-Converged Infrastructure (HCI) created by using the Dell EMC Solutions for Microsoft Azure Stack HCI. OMIMSWAC simplifies the tasks of IT administrators by remotely managing the PowerEdge servers and clusters throughout their life cycle.
BIOS	Basic Input or Output System. BIOS is firmware that is embedded on a small memory chip on the computer's system board or motherboard. It acts as an interface between the computer's hardware and the operating system. BIOS also contains instructions that the computer uses to perform basic instructions such as whether to boot from network or hard disk drive
Console	The management application a user utilizes to perform remote platform management tasks.
DRM—Dell EMC Repository Manager	Dell EMC Repository Manager (DRM) is an application within the Dell OpenManage portfolio that allows IT Administrators to easily manage system updates. Dell Repository Manager provides a searchable interface used to create custom software collections known as bundles and repositories of Dell Update Packages (DUPs).
DSU—Dell EMC System Update Utility	Dell EMC System Update (DSU) is a script-optimized update deployment tool for applying Dell Update Packages (DUP) to Dell EMC target nodes.
FQDN	Fully Qualified Domain Name.
Gateway administrators	Gateway administrators can configure who gets access as well as how users authenticate to the gateway. Only gateway administrators can view and configure the Access settings in Windows Admin Center. Local administrators on the gateway machine are always administrators of the Windows Admin Center gateway service.
Gateway system	Windows Admin Center installed as a gateway on a Windows server.
Gateway user	Gateway users can connect to the Windows Admin Center gateway service to manage servers through that gateway, but they can't change access permissions nor the authentication mechanism used to authenticate to the gateway.
Windows 10 gateway system	Windows Admin Center installed as a gateway on a Windows 10 OS.
HCI	Hyper-Converged Infrastructure.
IC—Dell EMC Inventory Collector	Inventory Collector is used to inventory the target system, compare the results against a Repository or Catalog and only deploy the updates that are required.
iDRAC	Integrated Dell Remote Access Controller.
IPMI	Intelligent Platform Management Interface
LED	Light Emitting Diode
NIC	Network Interface Card also known as Network Interface Controller

Table 4. Glossary (continued)

Abbreviations/ Acronyms	Definition
Offline - Dell EMC Repository Manager Catalog	Recommended when the DRM repositories are available in a shared location and is applicable for all managed devices by OMIMSWAC in data centers with no Internet connectivity.
Online (HTTPs) - Dell EMC Azure Stack HCI Solution Catalog	The firmware and driver update catalogs for Dell EMC Solutions for Azure Stack HCI catalog provides a catalog of all validated versions of the ready node and AHCI components. Recommended for Azure Stack HCI clusters (created using Dell EMC Microsoft Storage Spaces Direct Ready Nodes and Dell EMC appliance for Azure Stack HCI) and for Azure Stack HCI servers.
Online (HTTPs) - Dell EMC Enterprise Catalog	Recommended for PowerEdge servers.
Online (HTTPs) - Dell EMC MX Solution Catalog	Recommended for MX models of PowerEdge servers.
SATA	Serial Advanced Technology Attachment interface that is meant to replace the aging **PATA** technology.
USB	Universal Serial Bus
UI	User Interface
<Windows Directory>	C:\Windows

B

Appendix

While performing update compliance operation for SAS-RAID_Driver, ensure that *SATA controller* and *NVMe PCIe SSDs* are set to RAID mode. To configure RAID mode:

1. When the **Dell Power-On Self-Test (POST)** screen is displayed, press F2.

   Dell PowerEdge System Setup window is displayed.

   - Under **System BIOS setting** , configure RAID mode in **SATA settings** > **Embedded SATA**.
   - Under **System BIOS setting** , configure RAID mode in **NVMe settings** > **NVMe mode**.