Dell EMC OpenManage Integration 2.1 with Microsoft Windows Admin Center

Security Configuration Guide

D∕ELLEMC

Notes, cautions, and warnings

(i) **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

Tables

PREFACE

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document. This document was accurate at publication time. To ensure that you are using the latest version of this document, go to https://www.dell.com/support

Scope of the document

This document includes information about security features and capabilities of Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC). Also, use this document to:

● Understand the accessibility and data security of the extension.
● Know how to follow the recommendation/best practices of the extension to maximize the security posture in your environment.
● Understand the expectations to be fulfilled from security aspects for deploying OMIMSWAC.

Audience

This document is intended for individuals who are responsible for managing security for OMIMSWAC extension.

Document references

In addition to this guide, you can access other documents of OpenManage Integration with Microsoft Windows Admin Center available at **https://www.dell.com/support**.

● *Dell EMC OpenManage Integration with Microsoft Windows Admin Center Version 2.1 User's Guide*
● *Dell EMC OpenManage Integration for Microsoft Windows Admin Center Version 2.1 Release Notes*
● *Dell EMC OpenManage Integration for Microsoft Windows Admin Center Version 2.1 Installation Guide*
● *OpenManage Enterprise User's Guide*

Getting help

The Support website **https://www.dell.com/support** provides access to product licensing, documentation, advisories, downloads, and troubleshooting information. The information can enable you to resolve a product issue before you contact support.

1. Go to **https://www.dell.com/support**.
2. Select your support category.
3. Verify your country or region in the Choose a Country/Region drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to techpubcomments@dell.com.

Security quick reference

Topics:

- [Deployment models](#)
- [Security profiles](#)

Deployment models

You can download Dell EMC OpenManage Integration with Windows Admin Center from dell.com.

Prerequisites: Before you install OpenManage Integration version 2.1, ensure that you have installed the Windows Admin Center 2103.2 GA.

Microsoft Windows Admin Center (Microsoft WAC) is a locally deployed, browser-based app for managing Windows servers, clusters, hyper-converged infrastructure. To know how Microsoft Windows Admin Center supports different deployment model, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/deploy/prepare-environment. To know how Microsoft WAC supports deployment of extensions, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/extend/publish-extensions.

Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) is a Microsoft Windows Admin Center (Microsoft WAC) extension which inherits all the infrastructure services provided by the Microsoft WAC framework. For example, OMIMSWAC extension leverages the security services such as authorization, authentication, network security, and data security from Microsoft WAC framework.

The Dell EMC OpenManage Integration with Microsoft Windows Admin Center can be installed in one of the following methods:
- By using the Microsoft's public Windows Admin Center NuGet feed.
- By using a local path or a network share as package source for installation.
- By using the Microsoft Windows Admin Center workflow during Azure Stack HCI cluster deployment or updates.

After installation, OMIMSWAC appears as a Windows Admin Center extension.

To manage a cluster/server, connect to the cluster/server using "Manage as" option and provide appropriate cluster/server 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.

For more information about deploying OMIMSWAC extension, see the Dell EMC OpenManage Integration Version 2.1 with Microsoft Windows Admin Center Installation Guide available at https://www.dell.com/support.

Security profiles

OMIMSWAC runs under the default installation profile of Microsoft Windows Admin Center and security trust boundary. OMIMSWAC extension uses the same security profile as Windows Admin Center (https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/user-access-options).
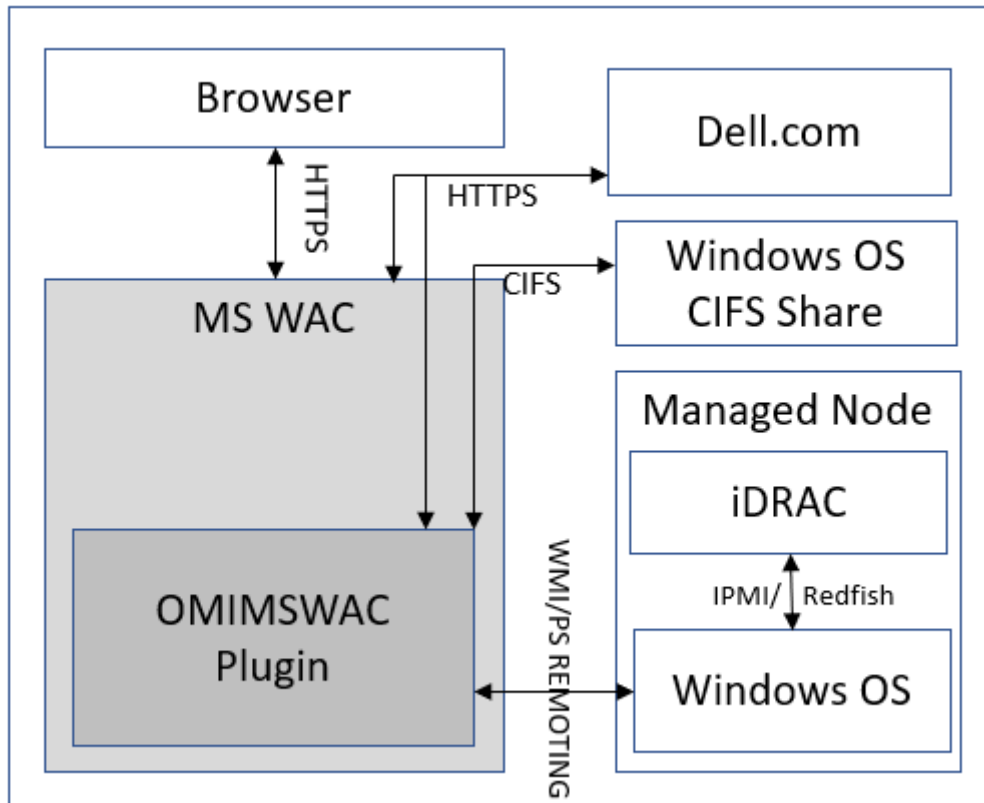
Product and subsystem security

Topics:

Security controls map

Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) is a Windows Admin Center extension which enables to manage:

- The PowerEdge servers as hosts
- Microsoft Failover Clusters created with PowerEdge servers
- Hyper-Converged Infrastructure (HCI)
- Dell EMC HCI Solutions for Microsoft Windows Server - created using the AX nodes and/or Storage Spaces Direct Ready Nodes
- Dell EMC Integrated System for Microsoft Azure Stack HCI - AX nodes

As the diagram depicts, OMIMSWAC interacts with `downloads.dell.com` through HTTPS protocol and with the network share through the CIFS.

OMIMSWAC does not store any credentials in any database or file storage. Secure session token is stored in browser cache and then it is discarded as soon as the session is invalidated. All accesses are managed by Microsoft Windows Admin Center (MS WAC) itself.

Authentication

Windows Admin Center user authentication

OMIMSWAC extension depends on authentication provided by the Windows Admin Center (https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/user-access-options) for managing/connecting to the target nodes. OMIMSWAC works only under a Gateway Administrator.

Login security settings

By default, Active Directory or local machine groups are used to control gateway access. If there is an Active Directory domain, user can manage gateway user and administrator access from within the Windows Admin Center interface.

Failed login behavior

Dell EMC OpenManage Integration is a tool extension used in Windows Admin Center. You can access the extension by logging into Windows Admin Center. For invalid credentials, Windows Admin Center does not allow to sign in and prompt again to enter valid credentials.

Authentication types and setup considerations

Authentication is inherited from the Windows Admin Center. There is no additional authentication supported by OMIMSWAC extension. It is managed by Windows Admin Center itself (for more details, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/configure/user-access-control)

For more information about Windows Admin Center authentication, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/user-access-options.

Authorization

OMIMSWAC inherits the authorization from the Windows Admin Center. OMIMSWAC extension works using administrative role only. Ensure that the administrator 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.

Once the administrator has logged into the Windows Admin Center, in the **Extensions** tab, the administrators can install, uninstall, or update gateway extensions.

The **Access** tab lets administrators configure who can access the Windows Admin Center gateway, as well as the identity provider used to authenticate users.

For managing the server/cluster, user can use **Manage As** credential. For OMIMSWAC extension, it is expected that user will use domain administrative credential to manage any server/cluster.

If read only users try to access OMIMSWAC, it will show an error:

```
Failed to retrieve the device inventory due to insufficient user privileges.
```

To access OMIMSWAC, make sure to login to Windows Admin Center using gateway administrator credentials. Then, connect the device from the Windows Admin Center using 'Manage As' option with administrator privileges.

For more details about Windows Admin Center authorization, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/configure/user-access-control.

Network security

OMIMSWAC extension operates within the trusted boundary of Windows Admin Center network security. The extension uses the Microsoft Windows Admin Center provided framework to secure data through HTTPS while communicating with target nodes. Windows Admin Center provides a mechanism to upload SSL certificate to secure the communication. The same communication channel is used by OMIMSWAC to communicate with target nodes. Some of the network security functionalities are mentioned below:

- OMIMSWAC downloads the artifacts and tools required for updating the server/cluster from `Downloads.dell.com` using HTTPS protocol.
- OMIMSWAC uses the WAC framework to connect to managed node(s) using the WMI/PowerShell Remoting.
- OMIMSWAC uses the IPMI command to enable the USB-NIC interface (also known as OS to IDRAC pass through in iDRAC) to establish a session (for Redfish channel creation) with iDRAC. Once the channel is created, it will connect to the target nodes using HTTPS protocols. OMIMSWAC also involves in connecting to iDRAC from the managed node through Redfish API using HTTPS protocol.

  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 (also known as OS to IDRAC pass through in iDRAC) and creating an iDRAC user on the target node. Click **Accept** to continue to manage the servers/clusters by using the OpenManage Integration. OMIMSWAC extension will use that channel to get inventory and license details from the iDRAC. If you do not click **Accept**, you will not be able to access the extension.

  If USB-NIC is disabled or redfish service is disabled at iDRAC, OMIMSWAC shows the error: `The Redfish service is not accessible because the USB NIC adapter is disabled on the target node OS or the Redfish service is not enabled on iDRAC. To manage the target node by using OpenManage Integration with Microsoft Windows Admin Center, ensure that the USB NIC adapter and Redfish service are enabled on target node.`

Network exposure

Table 1. Ports Windows Admin Center listens for connections

Port number	Type	Function	Configurable port	Maximum Encryption Level
6516 (default)(win 10) or 443 (default)(service mode)	TCP	HTTPS	Yes	256-bit SSL
445 For more information about the SMB port 445, see Port configuration on the target server in Microsoft document.	TCP	Common Internet File System (CIFS)/SMB (Server Message Block)	No	None

Data security

OMIMSWAC extension doesn't store any sensitive customer data.

However, only to support offline scenarios, OMIMSWAC leverages the Microsoft Windows Admin Center framework to store operational data (as mentioned below) in application settings. For more information, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/configure/settings.

Operational data such as catalog path, Dell System Update (DSU), and Inventory Collector (IC) path from the CIFS share location.

CIFS share access requires user credentials which are available in the current browser session. Credentials, in obfuscated format, are only available to the current user. Credentials are discarded as soon as the session is invalidated. User needs to provide credentials again to access the CIFS share.

Cryptography

OMIMSWAC extension doesn't store any sensitive data or any certificates.

Auditing and logging

The OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) extension logs for target nodes and cluster nodes are available at `<Windows Directory>\Temp\OMIMSWAC` on target nodes.

The application logs for the update compliance feature are 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`

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

When an online catalog source is selected, and if DSU and IC are not configured in advance in the settings, 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.

Serviceability

The support website https://www.dell.com/support provides access to licensing information, product documentation, advisories, and downloads, and troubleshooting information. This information may enable you to resolve a product issue before you contact Support.

Security updates and patches

A security update for OMIMSWAC extension will be available periodically and can be installed in one of the following methods:
● Microsoft's public Windows Admin Center NuGet feed—You can install the latest extension by using the NuGet feed of Microsoft Windows Admin Center.

   Windows Admin Center notifies users when there is an update available for the extension.

● Dell Support site—You can download and install the `Dell_EMC_OpenManage_Integration_MS_WAC_<Version>.<Build_Number>.zip` file from dell.com (online) or from an already downloaded package in a network share (offline).

Ensure that you install OMIMSWAC extension security patches and other updates when they are available. For more information, see OpenManage Integration with Microsoft Windows Admin Center Installation Guide.

Product code integrity

The Dell EMC OpenManage Integration with Microsoft Windows Admin Center package is signed by Dell. It is recommended that you verify the authenticity of the OpenManage Integration with Microsoft Windows Admin Center package. To ensure the integrity of your download, use SHA-256, SHA-1 and MD5 checksums.

Miscellaneous Configuration and Management Elements

Topics:

OpenManage Integration with Microsoft Windows Admin Center Licensing

This section provides licensing guidance for OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC).

Overview

Installing and using OMIMSWAC Base version does not require any license and can be downloaded from the NuGet feed of Microsoft Windows Admin Center or Dell support site. The Base version provides basic management and monitoring for Dell EMC PowerEdge Servers, AX nodes, and Storage Spaces Direct Ready Nodes from Dell Technologies. However, to use some of the premium features, such as Cluster-Aware Updating (CAU), Hardware symmetry checks using Integrated Cluster Deployment and Update (IDU), and Full Stack Cluster-Aware Updating you must install the OMIWAC Premium License on target nodes.

Types of premium licenses and platforms supported

There are two types of OMIWAC Premium Licenses currently available as below.

- The "OMIWAC **Premium License for PowerEdge**" is available for:
  - YX4X models of Dell EMC PowerEdge server and above with iDRAC firmware 4.00.00.00 or newer.
- The "OMIWAC **Premium License for MSFT HCI Solutions**" is available for:
  - AX nodes and Storage Space Direct Ready Nodes from Dell Technologies with firmware 4.00.00.00 or newer.
  - Dell EMC Integrated System for Microsoft Azure Stack HCI.
  - Dell EMC HCI Solutions for Microsoft Windows Server.

Premium features supported

- Cluster-Aware Updating feature is supported for:
  - Failover clusters
  - Azure Stack HCI clusters
  - Windows Server HCI clusters
- Integrated Cluster Deploy and Update as part of Azure Stack HCI cluster creation with hardware symmetry checks is supported for:
  - AX nodes while creating Azure Stack HCI cluster.
- Full Stack Cluster-Aware updating feature is supported for:
  - Azure Stack HCI cluster.
- CPU core management is supported for:
  - Azure Stack HCI cluster created from AX nodes from Dell Technologies.

- Windows Server HCI cluster created from AX and/or S2D ready nodes from Dell Technologies.
  - Individual nodes such as AX nodes, S2D ready nodes, and PowerEdge nodes.
- Preparing nodes for cluster expansion is supported for:
  - Azure Stack HCI cluster created from AX nodes from Dell Technologies.
  - Windows Server HCI cluster created from AX nodes from Dell Technologies.
  - Failover cluster.

Purchase OMIWAC Premium License

OMIWAC Premium Licenses can be purchased while ordering the corresponding servers and solutions through Point of Sale (POS) or After Point of Sale (APOS) by contacting Dell sales representatives. The OMIWAC Premium License is bundled as part of the server license if purchased along with the server. If the license is purchased in APOS method, import the license manually using the iDRAC. For more information about importing license manually, see iDRAC documentation.

(i) **NOTE:** Licenses must be purchased for the corresponding Azure Stack HCI or PowerEdge Servers in a cluster as follows where you want to use the premium feature. As, mixing the licenses will not be supported.

License	Description	Licensing model
iDRAC express	All base features.	
OMIWAC **Premium License for PowerEdge**.	All base features along with premium management features.	Perpetual iDRAC based license.
OMIWAC **Premium License for MSFT HCI Solutions**. This is also shown as "OMIWAC Premium License for Azure Stack HCI" in iDRAC.	All base features along with premium management features.	Perpetual iDRAC based license.

(i) **NOTE:** The OMIWAC Premium License is not required to update individual target node.

You can download the purchased license from the Software License Management Portal at HTTPS://WWW.DELL.COM/SUPPORT/SOFTWARE/US/EN/04.

Verify license information

In OMIMSWAC, you can view nodes details and their licenses from the iDRAC inventory. To view the iDRAC inventory of a target node
1. In Windows Admin Center, connect to a server or cluster.
2. In the left pane of Windows Admin Center, under EXTENSIONS, click **Dell EMC OpenManage Integration**, and then navigate to the **iDRAC** tab.
3. Under iDRAC tab, you can verify the OMIWAC Premium License available on the target nodes.

(i) **NOTE:** All nodes participating in the managed cluster must have OMIWAC Premium License installed to use premium features. If any of the cluster nodes are not licensed, OMIMSWAC notifies and does not allow you to use the premium feature.

Credential Security Service Provider (CredSSP)

To perform any cluster operation such as Clustered-Aware Updating (CAU) using OMIMSWAC, as per Microsoft Windows Admin Center recommendation, CredSSP needs to be enabled. The extension, when required, will prompt to enable the CredSSP. Click **Yes** to enable the CredSSP to continue with the operation.

OMIMSWAC extension uses the MS WAC framework API to enable the CredSSP as follow:
1. Enables the client role in the Gateway system.
2. Enables the server role in each of the node.

For more information on CredSSP, see https://docs.microsoft.com/en-us/windows/win32/secauthn/credential-security-support-provider.

When cluster is not in use, it is recommended to disable the credssp.

OS to iDRAC Pass through

While fetching inventory from the target node, OMIMSWAC extension enables the OS-to-iDRAC pass through for the very first time, if it is not enabled.

Protect authenticity and integrity

To ensure product integrity, the OMIMSWAC installation components are signed.

OMIMSWAC extension leverages the API provided by Microsoft while accessing and downloading components from https://downloads.dell.com and verifies the signature of all the components that are downloaded from https://downloads.dell.com.

Catalog (.gz file) and dependent update tools such as DSU and IC are expected to be signed before usage.

For DSU/IC with invalid signature, OMIMSWAC will show an error:

```
Signature verification for Inventory Collector (IC) or Dell System Update (DSU) failed.
Ensure the IC or DSU is downloaded from the location mentioned in the Compatibility
matrix of the OMIMSWAC Installation Guide. Error.
```

For catalog having invalid signature, OMIMSWAC will show an error:

```
The catalog file has invalid signature.
```

Manage backup and restore in OMIMSWAC

OMIMSWAC runs under Windows Admin Center and doesn't store any data. Backup and restore is not applicable.

Contacting Dell

Prerequisites

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

About this task

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

Steps

1. Go to **Dell.com/support**.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.