Dell OpenManage Integration with Microsoft Windows Admin Center version 3.1

Security Configuration Guide

June 2023
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

Tables

1

PREFACE

As part of an effort to improve its product lines, Dell Technologies 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 Technologies 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 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 OpenManage Integration with Microsoft Windows Admin Center User's Guide*
- *Dell OpenManage Integration for Microsoft Windows Admin Center Release Notes*

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

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

Before you install the latest version of OpenManage Integration extension, ensure that you have installed the Windows Admin Center 2211 GA.

Microsoft Windows Admin Center 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 OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) is a Microsoft Windows Admin Center 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 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 the extension is installed, 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 latest Dell OpenManage Integration with Microsoft Windows Admin Center user's 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).

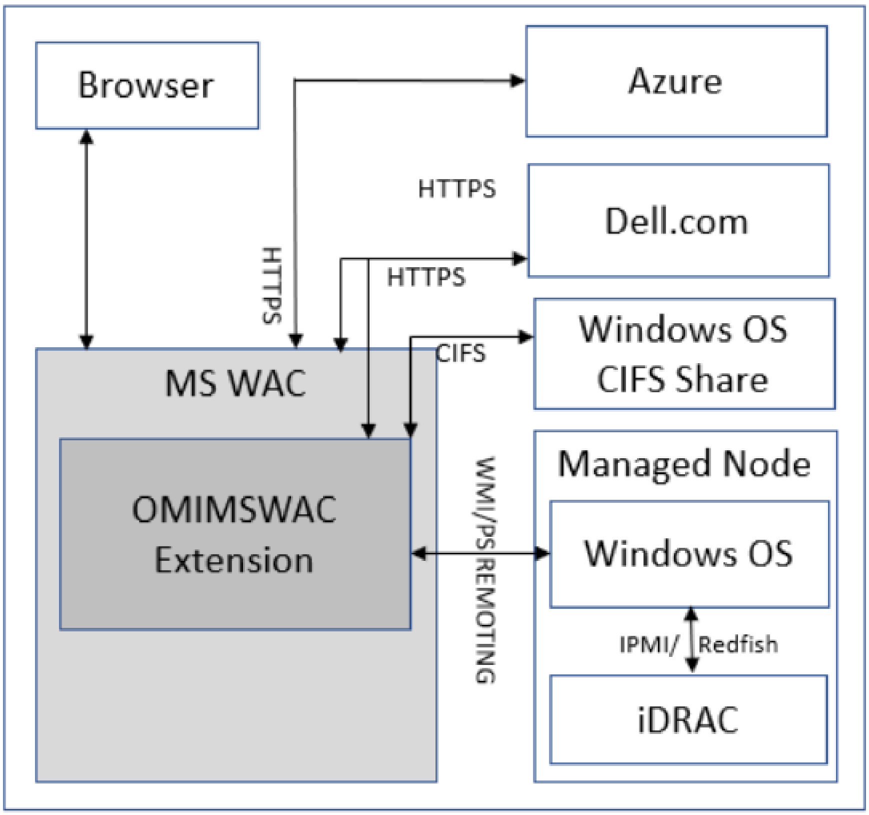
Product and subsystem security

Topics:

Security controls map

Dell 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* and Microsoft Azure portal 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 when the session is invalidated. Authentication to Azure is managed by Microsoft Windows Admin Center (MS WAC) SDK. All accesses are managed by Microsoft Windows Admin Center itself.

Authentication

Windows Admin Center user authentication

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

Authentication to Azure is managed by Microsoft Windows Admin Center SDK.

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.

All Azure flows require a valid token that is provided by Microsoft Windows Admin Center SDK after successful authentication.

Failed login behavior

Dell OpenManage Integration is a tool extension that is 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.

All Azure flows require a valid token, which is generated after successful authentication and not expired. For any unsuccessful authentication, the token cannot be generated and all subsequent Azure flows are denied. Users are informed about the unsuccessful authentication through notifications generated by Microsoft APIs.

Authentication types and setup considerations

Authentication to manage nodes is inherited from Windows Admin Center whereas Azure related service authentication is controlled from Windows Admin Center. There is no additional authentication that is supported by OMIMSWAC extension. It is managed by Windows Admin Center itself.

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 extension works using only the administrative role. 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, under **Settings**, in the **Extensions** tab, the administrators can install, uninstall, or update gateway extensions.

Under **Settings**, 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.

Below permission are required from Windows Admin Center to onboard policies into Azure.

- Microsoft.Authorization/policyassignments/
- Microsoft.Authorization/policydefinitions/
- Microsoft.Authorization/policyexemptions/
- Microsoft.Authorization/policysetdefinitions/

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.
- OMIMSWAC connects to Microsoft Azure portal 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.

NOTE:

- If you update servers or clusters using the "Run now" option, BitLocker on the operating system volume of Azure Stack HCI 22H2 is suspended during the reboot. After the update is complete, BitLocker is automatically enabled again.
- If you update clusters using the "Schedule update" option, BitLocker on the operating system volume of Azure Stack HCI 22H2 is suspended during the reboot. After the update is complete, BitLocker is automatically enabled again.
- If you update servers using the "Schedule update" option, BitLocker on the operating system volume of Azure Stack HCI 22H2 is suspended during the reboot. After the update is complete, enable the BitLocker manually. For more, see Suspend BitLocker protection for non-Microsoft software updates and Suspend-Bit Locker

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 and the sign in information for Azure 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_OpenManage_Integration_MS_WAC_<Version>.<Build_Number>.zip` file from www.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 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.

4

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 Windows Admin Center Azure DevOps feed or Dell support site. The Base version provides basic management and monitoring for Dell 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:
  - 14G or newer generations of Dell PowerEdge server 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 Integrated System for Microsoft Azure Stack HCI.
  - Dell HCI Solutions for Microsoft Windows Server.

Premium features supported

See the "Compatibility matrix" section in the User's Guide.

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 Technologies 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.

ⓘ **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.

ⓘ **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

1. In Windows Admin Center, connect to a server or cluster.
2. In the left pane of Windows Admin Center, under EXTENSIONS, click **Dell OpenManage Integration**.
3. Click **View** > **Overview**. For clusters, select a node from the **Node** drop-down. Node details along with OMIWAC Premium license status is displayed.

ⓘ **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.
```

NOTE: Sign-in verification is also done for support matrix, HCP metadata json, policy json, SCP metadata json, and HCP repository DSC module. These files are used during different work flows in OMIMSWAC.

Protect and secure your infrastructure

Protect your infrastructure with infrastructure lock

Infrastructure lock (also known as system lockdown mode) helps in preventing unintended changes after a system is provisioned. This feature blocks unintended changes to BIOS, iDRAC, firmware, and so on that helps you maintain the intended infrastructure configuration as it is. When the system is locked down, any attempt to change the system configuration and infrastructure related updates to BIOS, firmware, and drivers is blocked. This feature also allows administrators to disable the infrastructure lock for HCI and Failover clusters for the intended configuration and update to the cluster, and enables it back automatically after the operation is finished. For more information about this feature, see OMIMSWAC user's guide.

NOTE: Dell Technologies recommends that you enable the infrastructure lock to avoid any unintended changes to HCI and failover clusters.

Secure your infrastructure with secured-core

With this feature, you can protect your infrastructure (Failover clusters) from being compromised and ensure that your infrastructure boots using only software trusted by Dell Technologies.

NOTE: Dell Technologies and Microsoft recommend to enable Secured Core for Windows Server 2022 that includes both the Dell Infrastructure and Microsoft Operating System features to protect the infrastructure from external threats.

Secured-core feature in OpenManage Integration configures BIOS security features in Failover clusters in a cluster-aware manner.

OpenManage Integration leverages Windows Admin Center security extension tool to display the secured core status of clusters and cluster nodes at the Operating System level.

Secured-core feature in Microsoft enables dependent Operating System security features in Failover clusters.

For more information about this feature, see OMIMSWAC user's guide.

Manage backup and restore in OMIMSWAC

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

5

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.