Technical Whitepaper

Onboard Dell Server Configuration Profile Policies from Windows Admin Center to Azure Arc for PowerEdge Servers

Abstract

This white paper provides comprehensive guidance on onboarding Dell Server Configuration Profile (SCP) policies from Windows Admin Center to Azure Arc for PowerEdge server so that administrators can leverage those policies and monitor server compliance in Azure.

July 2023

Revisions

Date	Description
June 2023	Initial release

Acknowledgments

This paper was produced by the following:

Authors:

- Srikanth Kumar Kondru — Software Senior Engineer
- Support: Ajit Parhi

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third-party content is updated by the relevant third parties, this document will be revised accordingly.

Table of Contents

Acronyms

Acronyms	Expansion
iDRAC	Integrated Dell Remote Access Controller
OMIMSWAC	OpenManage Integration with Microsoft Windows Admin Center
MS API	Microsoft Application Programming Interface
SCP	Server Configuration Profile
XXg (ex.14g,15g)	XXth Generation of Dell PowerEdge Server Platforms
WS19	Windows Server 2019
WAC	Windows Admin Center
SCP	Server Configuration Profile

Executive Summary

This white paper walks you through the process of onboarding Server Configuration Profile (SCP) policies to Azure Arc using the OpenManage Integration extension. By doing so, you can effectively monitor server compliance using these policies in Azure.

Intended Audience

The intended audiences of this document are IT administrators who use OMIMSWAC to onboard SCP policies to Azure Arc to monitor PowerEdge servers.

1 Introduction

Azure Arc is the one of the primary management tools for resource management at cloud and hybrid platform. By using Azure Integration feature in OpenManage Integration extension, you can use Azure portal in addition to the on-premises management with Windows Admin Center for server monitoring.

Maintaining compliance with Dell SCP policies is crucial for administrators throughout the life cycle of PowerEdge servers. The Azure Integration feature is designed to assist administrators in this endeavor. With the help of OpenManage Integration extension, you can easily onboard Dell SCP policies to Azure Arc. This enables you leverage these policies and monitor server compliance in Azure.

Before getting started, make sure to review the prerequisites for this process. See Prerequisites.

To begin onboarding policies into Azure, see Onboarding policies into Azure.

If you want to export a report on the onboarded policies, see Export the Onboarded Policies Report.

In case you want to update your SCP policies, see Update SCP Policies.

Lastly, if you encounter any non-compliant SCP policies, see Remediate SCP Policies.

2 Prerequisites

Ensure your PowerEdge server meets the following prerequisites before you onboard SCP policies to Azure Arc:

- You have an Azure subscription.
- WAC gateway is registered into Azure. For more information, see Register Windows Admin Center gateway with Azure.
- Server is registered and connected to Azure Arc. For more information, see Microsoft document.
- Server is of PowerEdge server 14G and above models.
- Server has Windows Server 2016 or later versions of operating system.
- Server has a valid “OMIWAC Premium License” installed. For more information, see Verify License Details.
- Server should not be part of any cluster.

Note: If any of the prerequisite checks fail, OMIMSWAC blocks the onboarding policies to the Azure Arc. For more information, see Troubleshooting section 7.1.

2.1 Register Windows Admin Center gateway with Azure

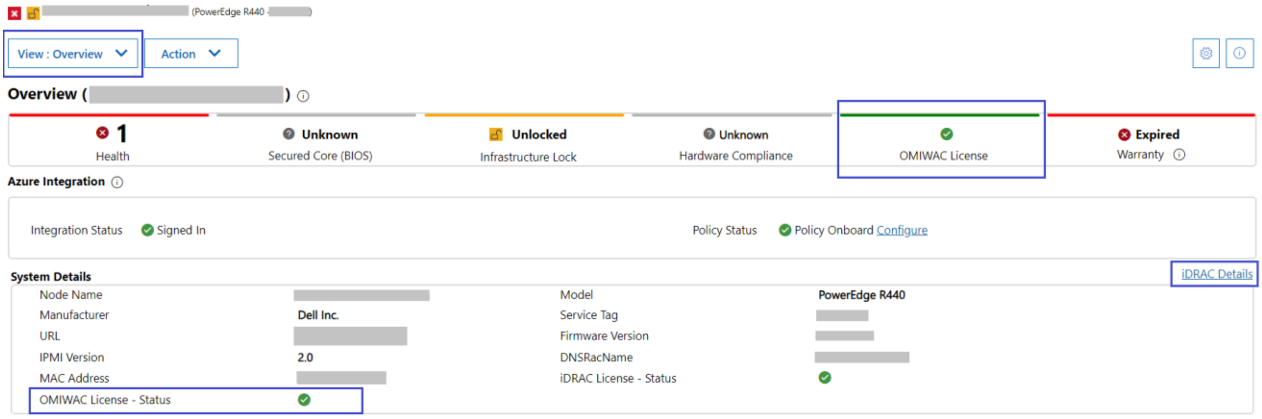
For information about registering Windows Admin Center with Azure, see Microsoft documents.

2.2 Verify license details

In OMIMSWAC, you can view node details and their licenses from the iDRAC inventory. The iDRAC inventory attributes are optimized to improve usability.

Perform the following steps to check license details:

1. In the Windows Admin Center, connect to a server or cluster.
2. In the left pane of the Windows Admin Center, under **EXTENSIONS**, click **Dell OpenManage Integration**.
3. In the **View** drop-down, select **Overview,** and then click the **iDRAC Details** link on the right-side corner of **System Details** section to view more about the license details.
4. To view the license details, click on a license attribute name. For example, iDRAC9 Enterprise License, OME Server Configuration Management, OMIWAC Premium License for PowerEdge, and more.



[redacted] (PowerEdge R440 [redacted])

Overview ([redacted])

1	Unknown	Unlocked	Unknown	✓	Expired
Health	Secured Core (BIOS)	Infrastructure Lock	Hardware Compliance	OMIWAC License	Warranty

Azure Integration

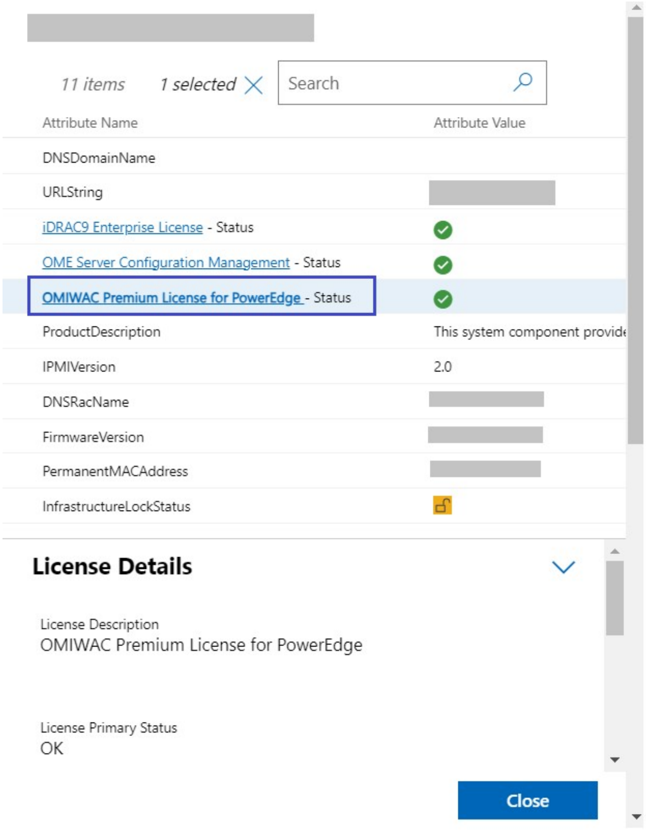
Integration Status ✓ Signed In

Policy Status ✓ Policy Onboard Configure

System Details

Node Name	[redacted]	Model	PowerEdge R440
Manufacturer	Dell Inc.	Service Tag	[redacted]
URL	[redacted]	Firmware Version	[redacted]
IPMI Version	2.0	DNSRacName	[redacted]
MAC Address	[redacted]	iDRAC License - Status	✓
OMIWAC License - Status	✓		

Figure 1: Verify license details from Overview page



[redacted]

Attribute Name	Attribute Value
DNSDomainName	
URLString	[redacted]
iDRAC9 Enterprise License - Status	✓
OME Server Configuration Management - Status	✓
OMIWAC Premium License for PowerEdge - Status	✓
ProductDescription	This system component provide
IPMIVersion	2.0
DNSRacName	[redacted]
FirmwareVersion	[redacted]
PermanentMACAddress	[redacted]
InfrastructureLockStatus	🔓

License Details

License Description
OMIWAC Premium License for PowerEdge

License Primary Status
OK

Figure 2: iDRAC details pop-up page

Note: Ensure that OMIWAC premium licenses are installed on all cluster nodes to use the Azure feature. For more information about OMIWAC premium licensing, see OMIMSWAC user's guide.

3 Onboard policies into Azure

In OMIMSWAC, when you click **Azure Integration** in the **View** drop-down menu, the extension checks if your server meets all the prerequisites that are mentioned in the previous section. If the prerequisites are satisfied, you can proceed with onboarding the policies.

To onboard policies into Azure, perform the following steps:

Step 1: Sign-In to Azure

Step 2: Onboarding Checklist

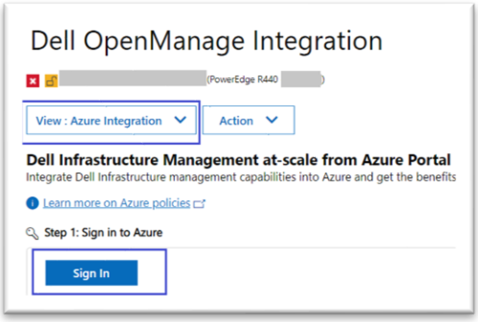
Step 3: Onboard Policies

3.1 Sign-In to Azure

Perform the following steps to sign-in to Azure:

1. In the **View** drop-down, click **Azure Integration**.
2. Click **Sign In.** A Sign in pop-up window appears. For more information, see Microsoft document.

- Once the signing is done, the status changes to **Signed In**.
- If the user had already signed-in to azure, then also status is shown as **Signed In**.



Dell OpenManage Integration

[redacted] (PowerEdge R440 [redacted])

Dell Infrastructure Management at-scale from Azure Portal

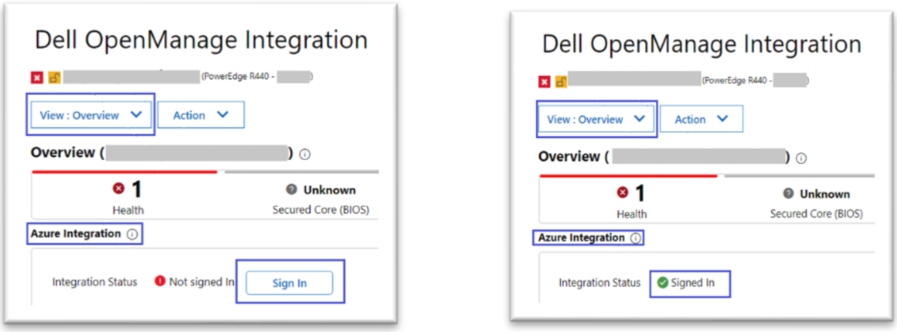
Integrate Dell Infrastructure management capabilities into Azure and get the benefits

Learn more on Azure policies

Step 1: Sign in to Azure

Figure 3: Sign-in

Note: Alternatively, you can also sign in to Azure from the **Overview** page. In **Azure Integration** section, click **Sign-in** to go to the Azure integration page. Sign-in pop-up window appears for you to sign in to the Azure.



Dell OpenManage Integration

[redacted] (PowerEdge R440 - [redacted])

Overview ([redacted])

1 Health

Unknown Secured Core (BIOS)

Azure Integration

Integration Status: Not signed In

Dell OpenManage Integration

[redacted] (PowerEdge R440 - [redacted])

Overview ([redacted])

1 Health

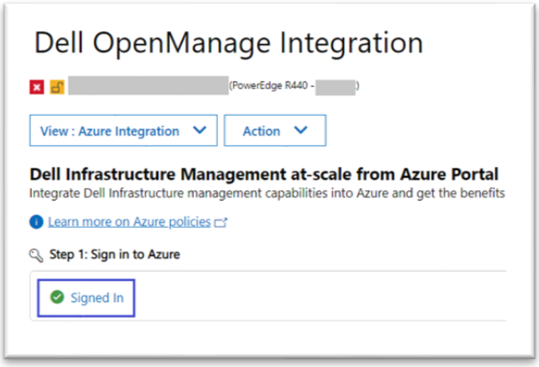
Unknown Secured Core (BIOS)

Azure Integration

Integration Status: Signed In

Figure 4: Sign-In from Overview page (before and after Sign-In status)

Once you have signed-In, **step 2: Onboarding Checklist** section is enabled.



Dell OpenManage Integration

[redacted] (PowerEdge R440 - [redacted])

Dell Infrastructure Management at-scale from Azure Portal

Integrate Dell Infrastructure management capabilities into Azure and get the benefits

Learn more on Azure policies

Step 1: Sign in to Azure

Figure 5: Sign-in status

Note: Sign-in to Azure is handled by Microsoft Windows Admin Center APIs and Dell extension does not have any control over it.

3.2 Onboarding checklist

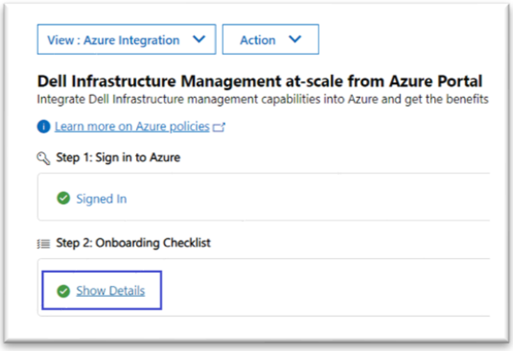
After the **step 2: Onboarding Checklist** is enabled, OMIMSWAC verifies the following requirements to ensure that both the user and the cluster are ready for onboarding policies:

User must have the following permissions to successfully onboard the SCP policies into Azure. These permissions include the ability to:

- create and manage policy assignments
- create and manage policy definitions
- create and manage policy exemptions
- create and manage policy sets

For more information about roles, see Microsoft document.
Ensure server is assigned to the registered resource group and the same resource group is not deleted in the Azure.

After all the onboarding checklists are met, the next **step 3: Onboard Policies** is enabled.



Dell Infrastructure Management at-scale from Azure Portal

Integrate Dell Infrastructure management capabilities into Azure and get the benefits

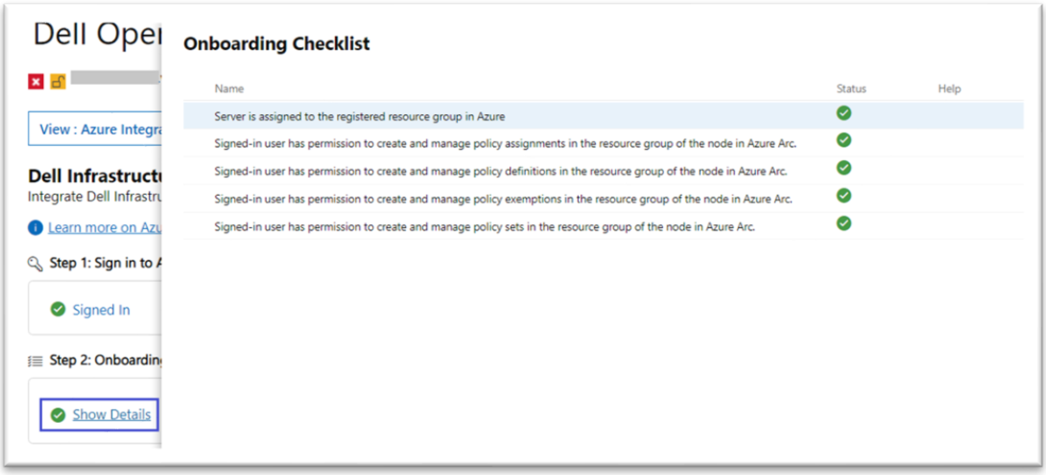
Learn more on Azure policies

Step 1: Sign in to Azure

Step 2: Onboarding Checklist

Figure 6: Onboarding check list show details

Click **Show Details** to see the list of checklists and their status.



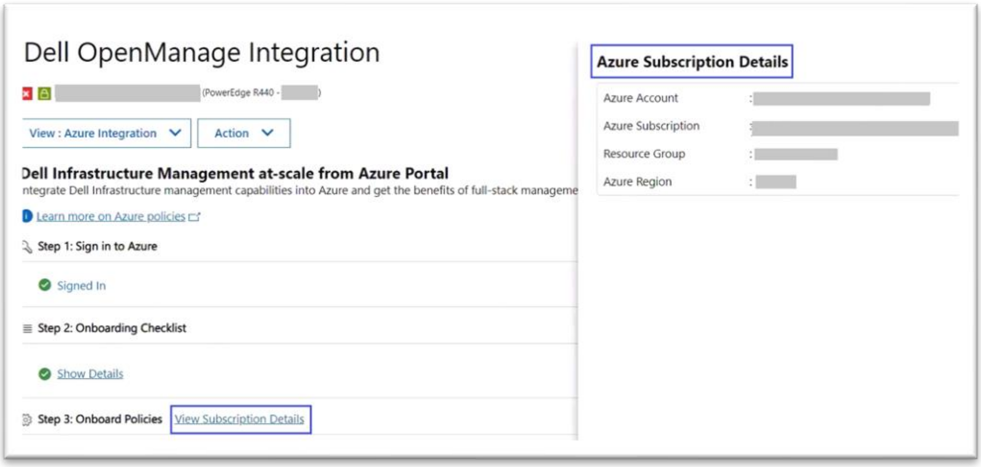
Onboarding Checklist

Name	Status	Help
Server is assigned to the registered resource group in Azure	✓	
Signed-in user has permission to create and manage policy assignments in the resource group of the node in Azure Arc.	✓	
Signed-in user has permission to create and manage policy definitions in the resource group of the node in Azure Arc.	✓	
Signed-in user has permission to create and manage policy exemptions in the resource group of the node in Azure Arc.	✓	
Signed-in user has permission to create and manage policy sets in the resource group of the node in Azure Arc.	✓	

Figure 7: Onboarding checklist pop-up page

3.3 Onboard policies

After the **Step 3: Onboard Policies** is enabled, click **View Subscription Details** to view the subscription and resource group info.

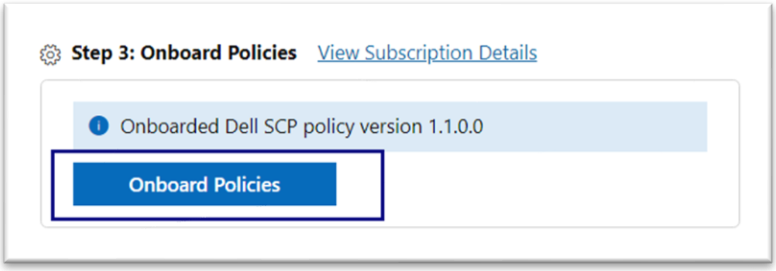

Dell OpenManage Integration
[redacted] (PowerEdge R440 - [redacted])
View : Azure Integration
Action
Dell Infrastructure Management at-scale from Azure Portal
ntegrate Dell Infrastructure management capabilities into Azure and get the benefits of full-stack manageme
Learn more on Azure policies
Step 1: Sign in to Azure
Signed In
Step 2: Onboarding Checklist
Show Details
Step 3: Onboard Policies
View Subscription Details

Azure Subscription Details

Azure Account	: [redacted]
Azure Subscription	: [redacted]
Resource Group	: [redacted]
Azure Region	: [redacted]

Figure 8: View subscription details

After the policies are fetched, **Onboard Policies** button is enabled.



Onboarded Dell SCP policy version 1.1.0.0

Figure 9: Onboard Policies

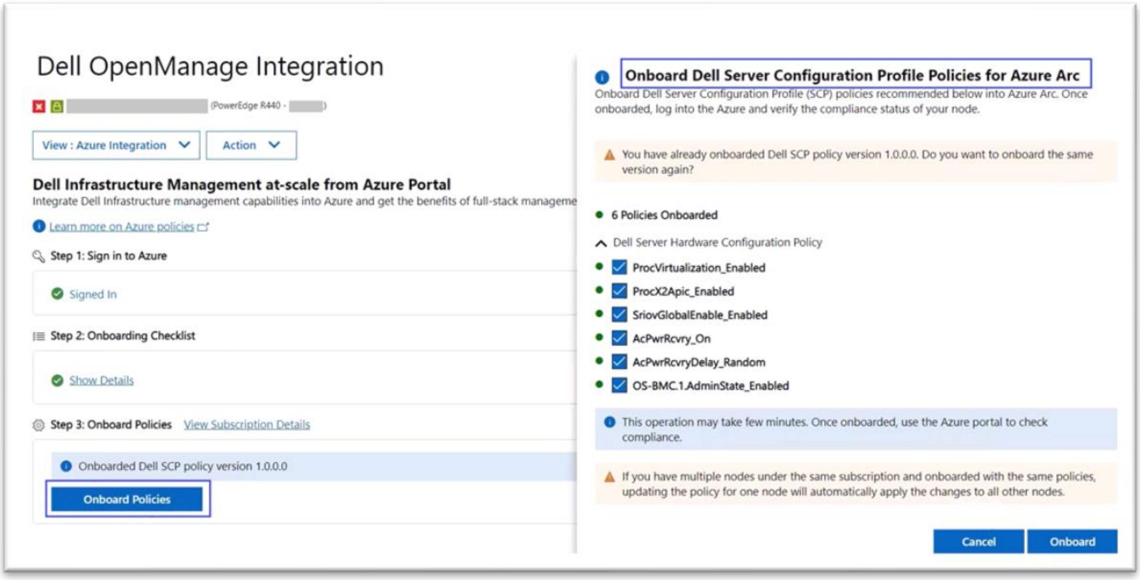
Click **Onboard Policies** to view the applicable policies for upload.
Onboard Dell Server Configuration Profile Policies for Azure Arc pane appears on the right. In this pane, the following policy category is shown:

- Dell Server Hardware configuration policy: This policy checks whether the server has Dell Technologies recommended BIOS, and iDRAC configurations.

  Checks are sub-categoried into:

  1. BIOS policy
     - ProcVirtualization_Enabled
     - ProcX2Apic_Enabled
     - SriovGlobalEnable_Enabled
     - AcPwrRcvry_On
     - AcPwrRcvryDelay_Random
  2. iDRAC policy
     - OS-BMC.1.AdminState_Enabled

All policies are shown as selected, and you can choose the policies based on your requirements.



Dell OpenManage Integration

[redacted] (PowerEdge R440 - [redacted])

Dell Infrastructure Management at-scale from Azure Portal
Integrate Dell Infrastructure management capabilities into Azure and get the benefits of full-stack manageme

Step 1: Sign in to Azure

✓ Signed In

Step 2: Onboarding Checklist

Step 3: Onboard Policies

Onboarded Dell SCP policy version 1.0.0.0

Onboard Dell Server Configuration Profile Policies for Azure Arc
Onboard Dell Server Configuration Profile (SCP) policies recommended below into Azure Arc. Once onboarded, log into the Azure and verify the compliance status of your node.

You have already onboarded Dell SCP policy version 1.0.0.0. Do you want to onboard the same version again?

● 6 Policies Onboarded

Dell Server Hardware Configuration Policy

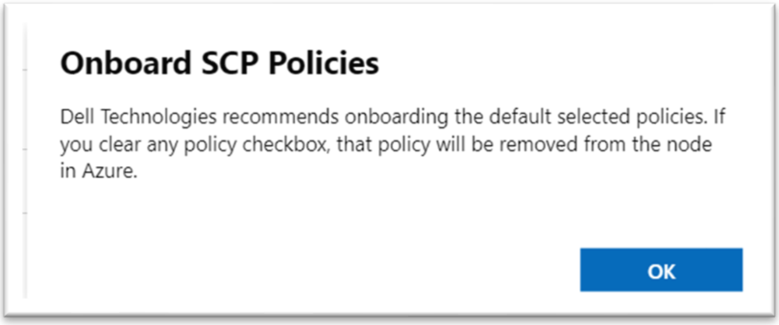
- ☑ ProcVirtualization_Enabled
- ☑ ProcX2Apic_Enabled
- ☑ SriovGlobalEnable_Enabled
- ☑ AcPwrRcvry_On
- ☑ AcPwrRcvryDelay_Random
- ☑ OS-BMC.1.AdminState_Enabled

This operation may take few minutes. Once onboarded, use the Azure portal to check compliance.

If you have multiple nodes under the same subscription and onboarded with the same policies, updating the policy for one node will automatically apply the changes to all other nodes.

Figure 10: Onboard policies

If you clear the selected policy for the first time, an alert popup will appear, as shown below.

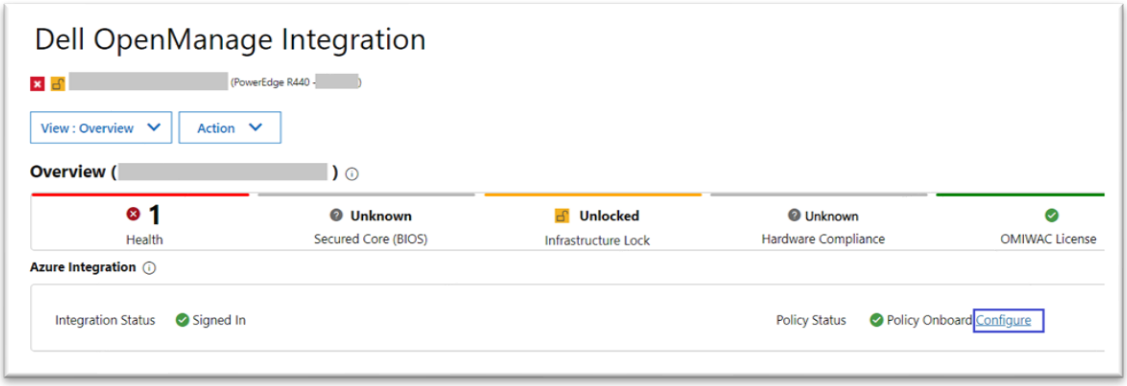


Onboard SCP Policies

Dell Technologies recommends onboarding the default selected policies. If you clear any policy checkbox, that policy will be removed from the node in Azure.

Figure 11: Policy uncheck alert pop-up

Note: Alternatively, you can also click the **Configure** link from the **Overview** page which will redirect to "**Onboard Dell Server Configuration Profile Policies for Azure Arc**" popup window in Azure page.



Dell OpenManage Integration

[redacted] (PowerEdge R440 - [redacted])

Overview ([redacted])

⊗ 1	Unknown	Unlocked	Unknown	✓
Health	Secured Core (BIOS)	Infrastructure Lock	Hardware Compliance	OMIWAC License

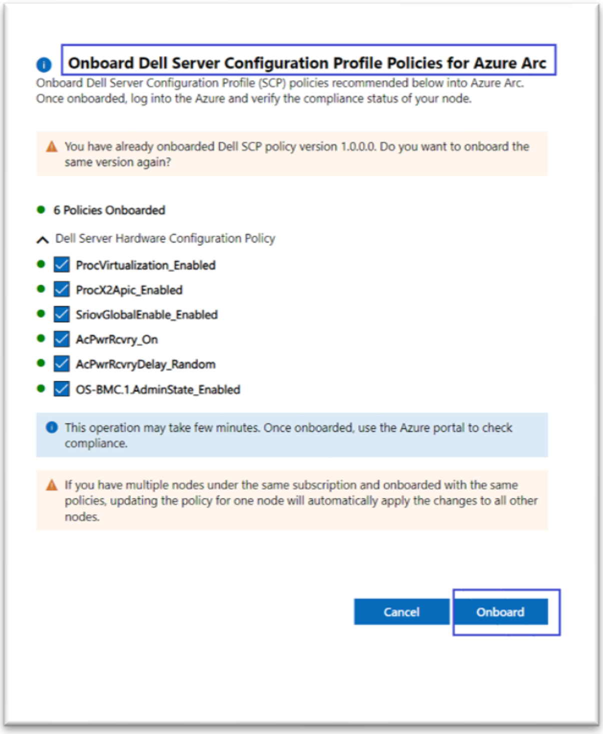
Azure Integration

Integration Status ✓ Signed In

Policy Status ✓ Policy Onboard Configure

Figure 12: Configure link from Overview page

1. Click **Onboard** to onboard the policies into Azure.



Onboard Dell Server Configuration Profile Policies for Azure Arc

Onboard Dell Server Configuration Profile (SCP) policies recommended below into Azure Arc. Once onboarded, log into the Azure and verify the compliance status of your node.

You have already onboarded Dell SCP policy version 1.0.0.0. Do you want to onboard the same version again?

- 6 Policies Onboarded

Dell Server Hardware Configuration Policy

- ☑ ProcVirtualization_Enabled
- ☑ ProcX2Apic_Enabled
- ☑ SriovGlobalEnable_Enabled
- ☑ AcPwrRcvry_On
- ☑ AcPwrRcvryDelay_Random
- ☑ OS-BMC.1.AdminState_Enabled

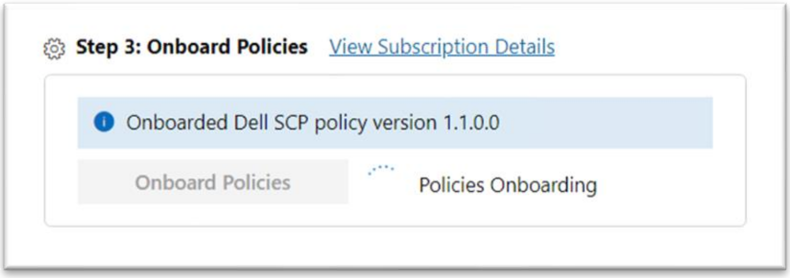
This operation may take few minutes. Once onboarded, use the Azure portal to check compliance.

If you have multiple nodes under the same subscription and onboarded with the same policies, updating the policy for one node will automatically apply the changes to all other nodes.

Figure 13: Onboard Dell Server Configuration Profile Policies to Azure Arc

Note: If you have multiple nodes under the same subscription and onboarded with the same policies, updating the policy for one node will automatically apply the changes to all other nodes.

After you click **Onboard**, the popup closes and the onboarding of the policies to Azure begins. Policies are created in Azure, along with their corresponding policy definitions and assignments.

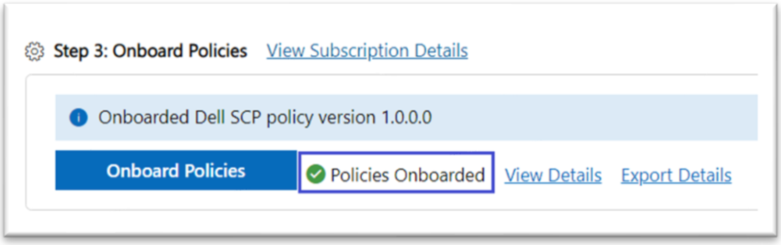


Step 3: Onboard Policies View Subscription Details

Onboarded Dell SCP policy version 1.1.0.0

Figure 14: Onboarding Policies

2. After the onboarding is complete, **View Details** and **Export Details** links appear.
   If success or failure, you receive notifications along with additional context to understand the status better.

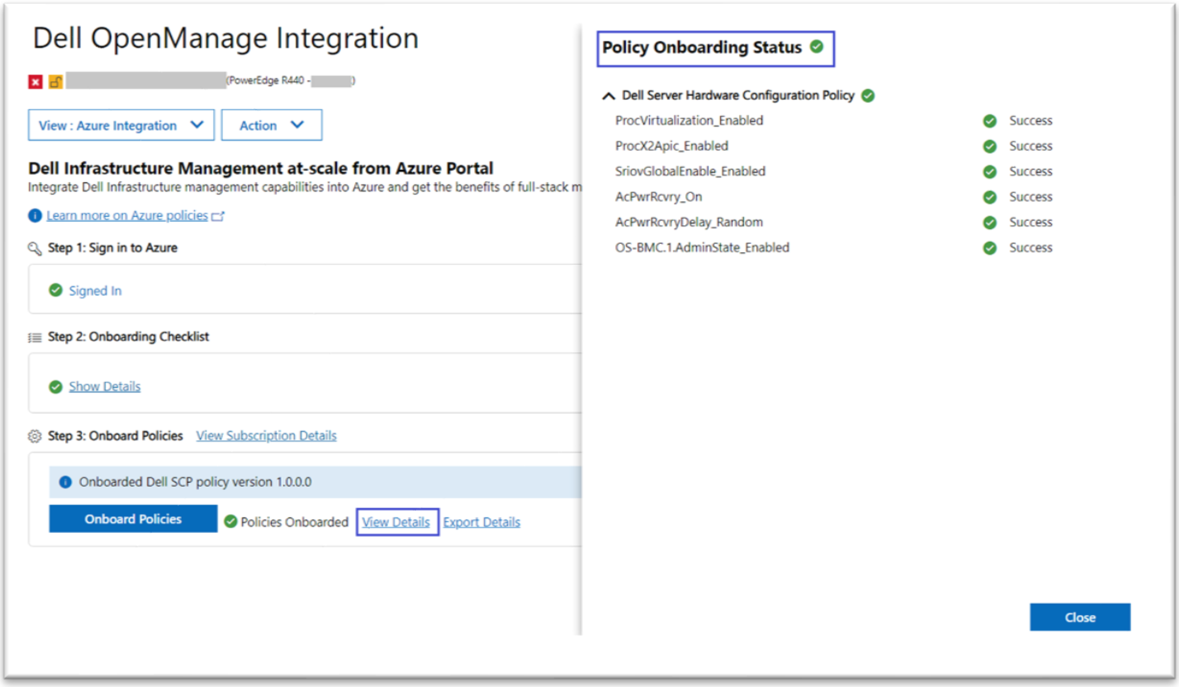


Step 3: Onboard Policies View Subscription Details

Onboarded Dell SCP policy version 1.0.0.0

Figure 15: Policies Onboarded- status

3. Click **View Details** to view the details of each policy creation and assignments status.



Dell OpenManage Integration

[redacted] (PowerEdge R440 - [redacted])

Dell Infrastructure Management at-scale from Azure Portal

Integrate Dell Infrastructure management capabilities into Azure and get the benefits of full-stack m

Learn more on Azure policies

Step 1: Sign in to Azure

✓ Signed In

Step 2: Onboarding Checklist

✓ Show Details

Step 3: Onboard Policies View Subscription Details

Onboarded Dell SCP policy version 1.0.0.0

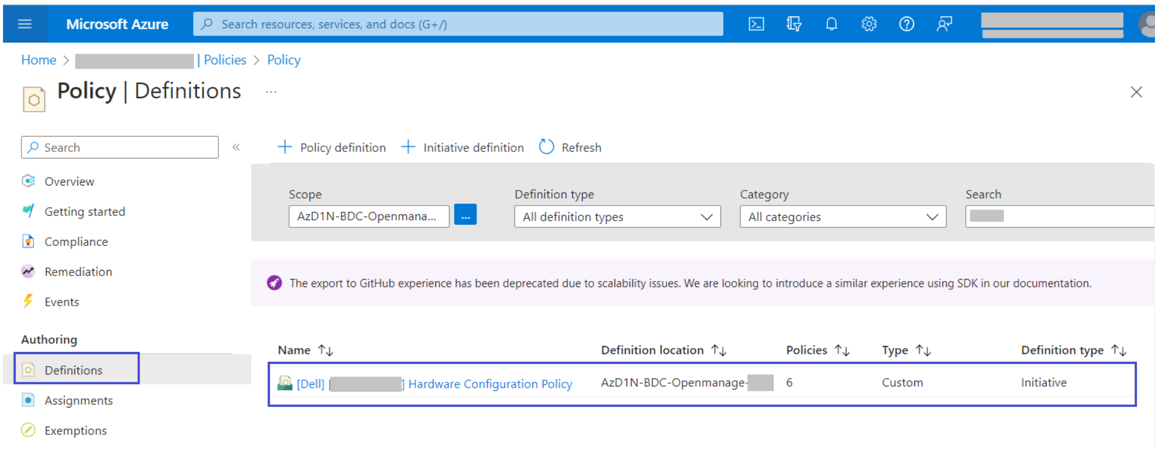
Policy Onboarding Status ✓

Dell Server Hardware Configuration Policy ✓

ProcVirtualization_Enabled	✓ Success
ProcX2Apic_Enabled	✓ Success
SriovGlobalEnable_Enabled	✓ Success
AcPwrRcvry_On	✓ Success
AcPwrRcvryDelay_Random	✓ Success
OS-BMC.1.AdminState_Enabled	✓ Success

Figure 16: Policies Onboarded- View Details

Once the policies are successfully onboarded to Azure, you can view the onboarded policies in the Azure portal. For more information, see Microsoft document.



Home > [redacted] | Policies > Policy

Policy | Definitions

Scope: AzD1N-BDC-Openmana...

Definition type: All definition types

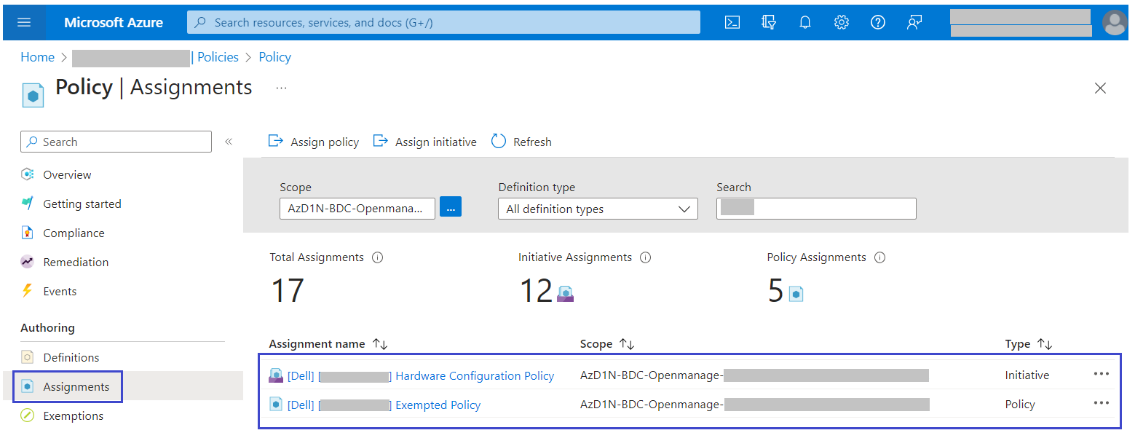
Category: All categories

Search: [redacted]

The export to GitHub experience has been deprecated due to scalability issues. We are looking to introduce a similar experience using SDK in our documentation.

Name	Definition location	Policies	Type	Definition type
[Dell] [redacted] Hardware Configuration Policy	AzD1N-BDC-Openmanage-[redacted]	6	Custom	Initiative

Figure 17: Policy definition in Azure portal



Home > [redacted] | Policies > Policy

Policy | Assignments

Scope: AzD1N-BDC-Openmana...

Definition type: All definition types

Search: [redacted]

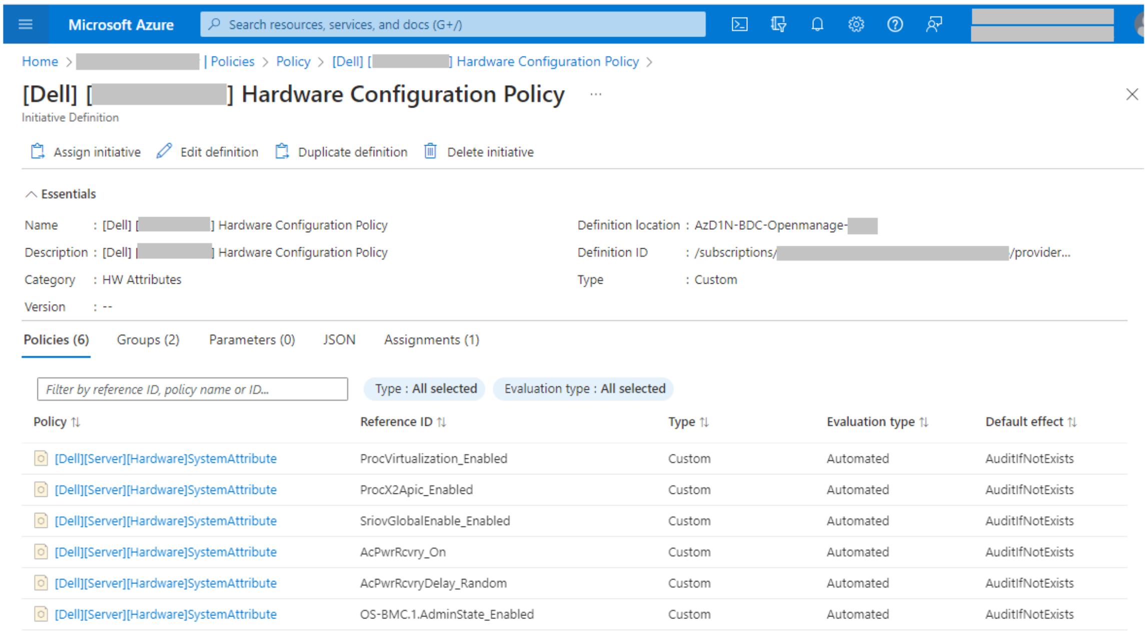
Total Assignments 17

Initiative Assignments 12

Policy Assignments 5

Assignment name	Scope	Type
[Dell] [redacted] Hardware Configuration Policy	AzD1N-BDC-Openmanage-[redacted]	Initiative
[Dell] [redacted] Exempted Policy	AzD1N-BDC-Openmanage-[redacted]	Policy

Figure 18: Policy assignment in Azure Portal



Home > [redacted] | Policies > Policy > [Dell] [redacted] Hardware Configuration Policy >

[Dell] [redacted] Hardware Configuration Policy

Initiative Definition

Name : [Dell] [redacted] Hardware Configuration Policy

Description : [Dell] [redacted] Hardware Configuration Policy

Category : HW Attributes

Version : --

Definition location : AzD1N-BDC-Openmanage-[redacted]

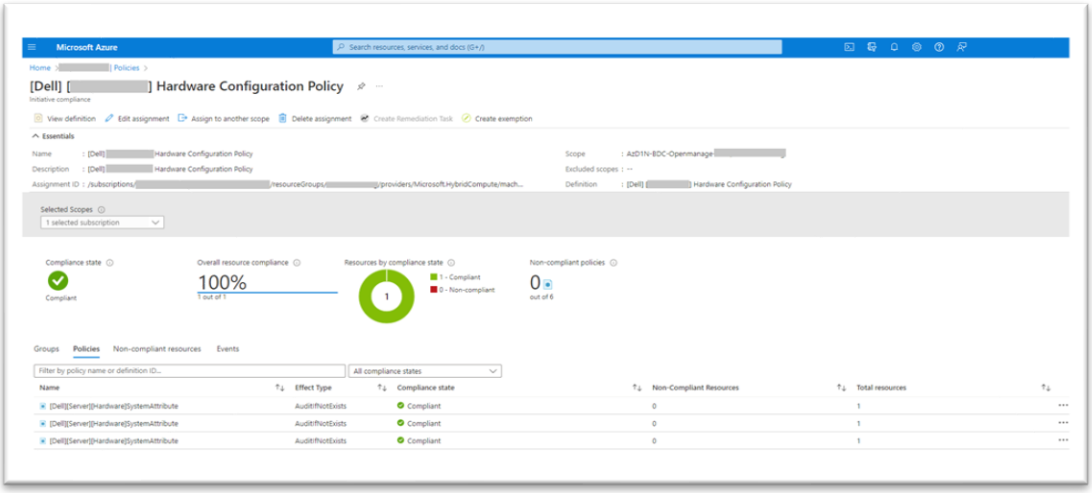
Definition ID : /subscriptions/[redacted]/provider...

Type : Custom

Policies (6)
Groups (2)
Parameters (0)
JSON
Assignments (1)
Filter by reference ID, policy name or ID...
Type : All selected
Evaluation type : All selected

Policy	Reference ID	Type	Evaluation type	Default effect
[Dell][Server][Hardware]SystemAttribute	ProcVirtualization_Enabled	Custom	Automated	AuditIfNotExists
[Dell][Server][Hardware]SystemAttribute	ProcX2Apic_Enabled	Custom	Automated	AuditIfNotExists
[Dell][Server][Hardware]SystemAttribute	SriovGlobalEnable_Enabled	Custom	Automated	AuditIfNotExists
[Dell][Server][Hardware]SystemAttribute	AcPwrRcvry_On	Custom	Automated	AuditIfNotExists
[Dell][Server][Hardware]SystemAttribute	AcPwrRcvryDelay_Random	Custom	Automated	AuditIfNotExists
[Dell][Server][Hardware]SystemAttribute	OS-BMC.1.AdminState_Enabled	Custom	Automated	AuditIfNotExists

Figure 19: SCP policy details in Azure portal



[Dell] [[redacted]] Hardware Configuration Policy

Initiative compliance

Name : [Dell] [redacted] Hardware Configuration Policy

Description : [Dell] [redacted] Hardware Configuration Policy

Assignment ID : /subscriptions/[redacted]/resourceGroups/[redacted]/providers/Microsoft.HybridCompute/mach...

Scope : AzD1N-BDC-Openmanage-[redacted]

Excluded scopes : --

Definition : [Dell] [redacted] Hardware Configuration Policy

Compliance state: Compliant

Overall resource compliance: 100% 1 out of 1

Resources by compliance state: 1

🟩 1 - Compliant

🟥 0 - Non-compliant

Non-compliant policies: 0 out of 6

Name	Effect Type	Compliance state	Non-Compliant Resources	Total resources
[Dell][Server][Hardware]SystemAttribute	AuditIfNotExists	✓ Compliant	0	1
[Dell][Server][Hardware]SystemAttribute	AuditIfNotExists	✓ Compliant	0	1
[Dell][Server][Hardware]SystemAttribute	AuditIfNotExists	✓ Compliant	0	1

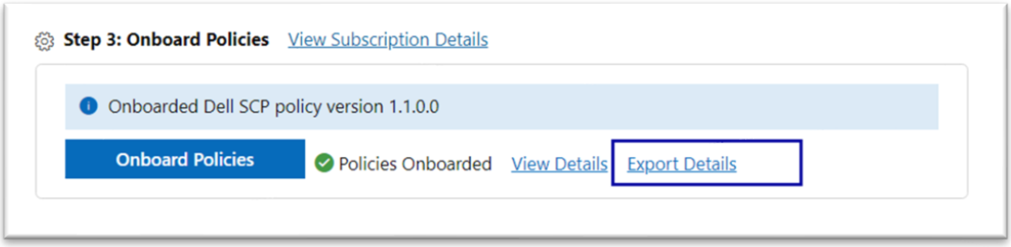
Figure 20: Policy compliance in Azure portal

Note: The policy compliance report is available on Azure Arc as well as in the OMIMSWAC Confguration Recommendation page, providing a consistent management experience.

4 Export the onboarded policies report

Once the policies are successfully onboarded to Azure Arc (As mentioned in section 3.1 to 3.3), you can export the details of the onboarded policies in an Excel (.xls) file.

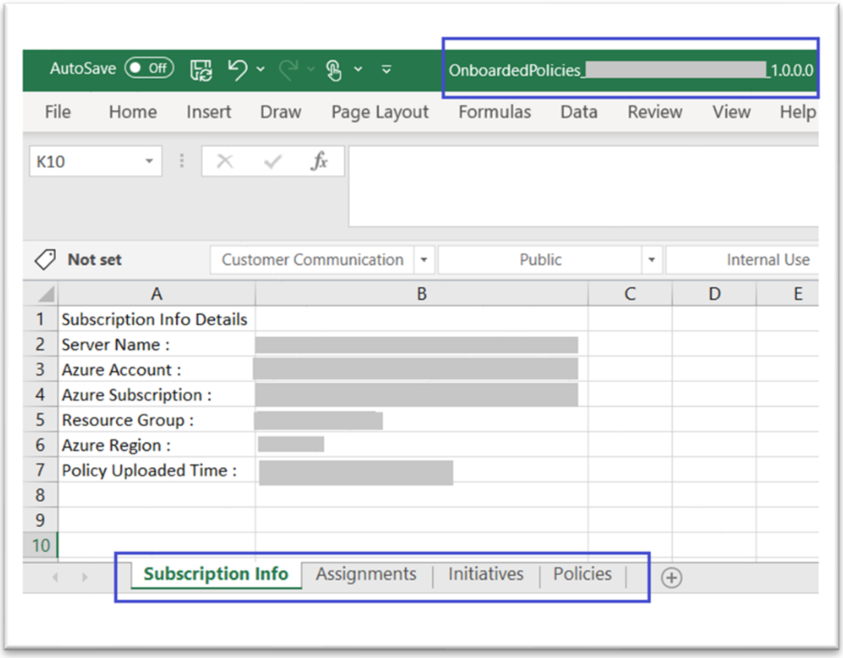
Click **Export Details** to download the details.



Step 3: Onboard Policies View Subscription Details

Onboarded Dell SCP policy version 1.1.0.0

Figure 21: Export details



OnboardedPolicies_[redacted]1.0.0.0

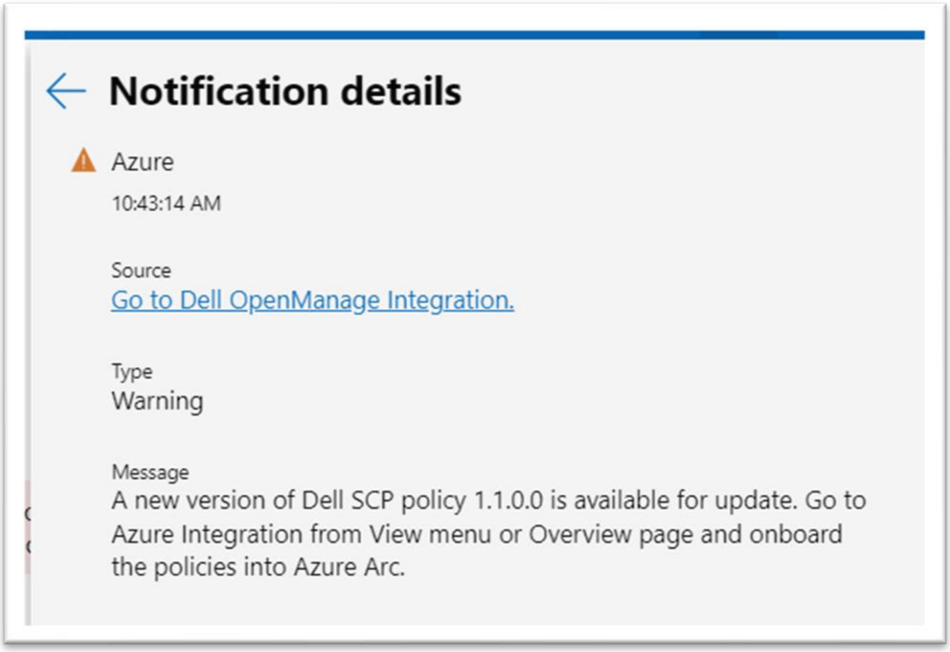
	A	B	C	D	E
1	Subscription Info Details				
2	Server Name :	[redacted]			
3	Azure Account :	[redacted]			
4	Azure Subscription :	[redacted]			
5	Resource Group :	[redacted]			
6	Azure Region :	[redacted]			
7	Policy Uploaded Time :	[redacted]			
8					
9					
10					

Figure 22: Export details – Excel file

5 Onboard updated SCP policies

After policies are onboarded in Azure Arc, it’s essential to keep the policies up to date. In OMIMSWAC, you receive a notification whenever a new version of the policy is available. To update the policy, click "**Onboard Policies**".

Note: If a new version of Dell SCP policy is available, you receive a notification with a message stating "*A new version of Dell SCP policy <version number> is available for update. Go to Azure Integration from View menu or Overview page and onboard the policies into Azure Arc.*"



Azure

10:43:14 AM

Source

Go to Dell OpenManage Integration.

Type

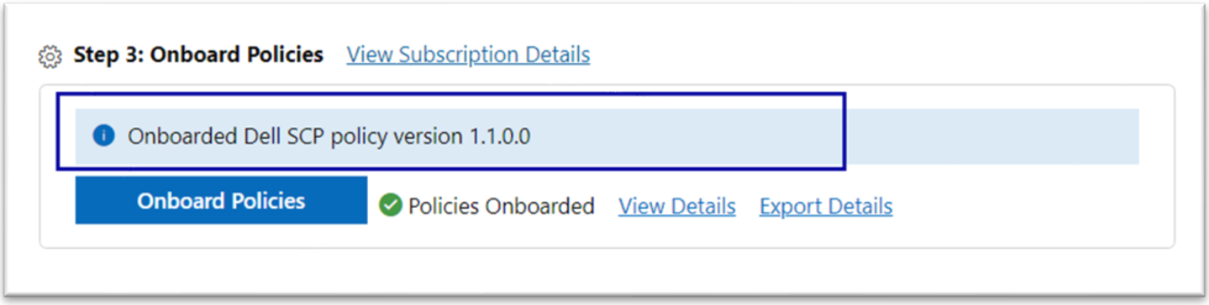
Warning

Message

A new version of Dell SCP policy 1.1.0.0 is available for update. Go to Azure Integration from View menu or Overview page and onboard the policies into Azure Arc.

Figure 23: Notification for new SCP policy version

When a new version of the onboarded policy is available, a notification appears. Follow the steps mentioned in section 3 and click **Onboard Policies**. The version of the policy, which is currently present in Azure, is displayed in **Step 3: Onboarded Policies** section.

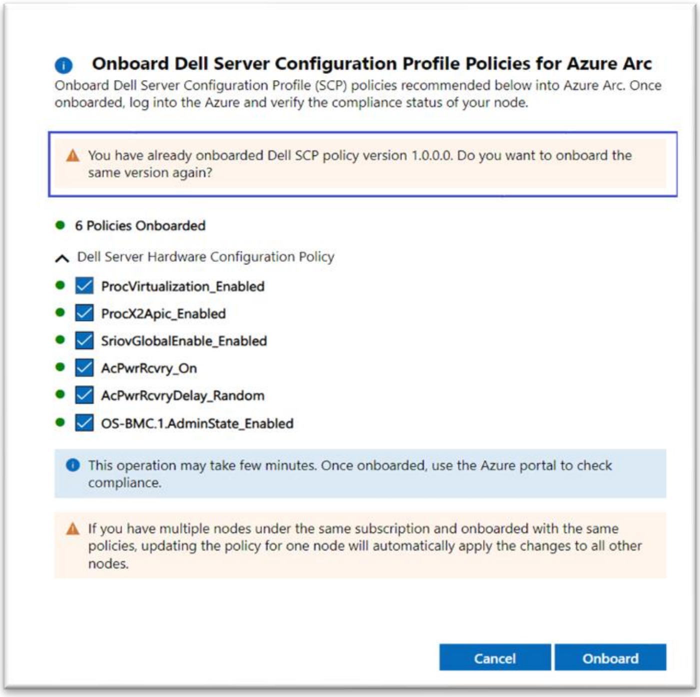


Onboarded Dell SCP policy version 1.1.0.0

Policies Onboarded

Figure 24: SCP Policy Version

Onboard Dell Server Configuration Profile Policies for Azure Arc pane appears on the right. View the version details of the policy being uploaded.



Onboard Dell Server Configuration Profile Policies for Azure Arc

Onboard Dell Server Configuration Profile (SCP) policies recommended below into Azure Arc. Once onboarded, log into the Azure and verify the compliance status of your node.

⚠ You have already onboarded Dell SCP policy version 1.0.0.0. Do you want to onboard the same version again?

● 6 Policies Onboarded

Dell Server Hardware Configuration Policy

- ● ☑ ProcVirtualization_Enabled
- ● ☑ ProcX2Apic_Enabled
- ● ☑ SriovGlobalEnable_Enabled
- ● ☑ AcPwrRcvry_On
- ● ☑ AcPwrRcvryDelay_Random
- ● ☑ OS-BMC.1.AdminState_Enabled

This operation may take few minutes. Once onboarded, use the Azure portal to check compliance.

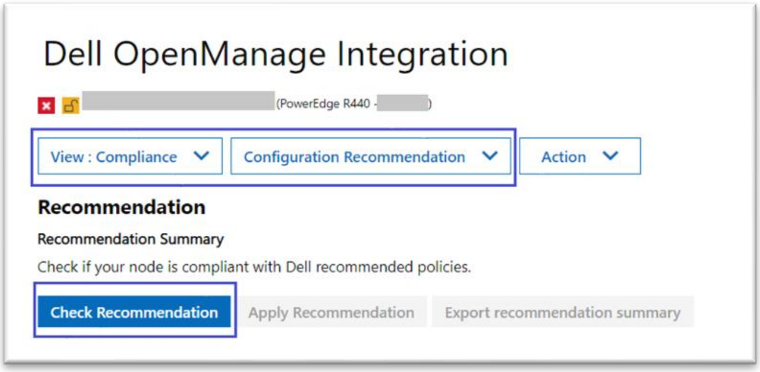
⚠ If you have multiple nodes under the same subscription and onboarded with the same policies, updating the policy for one node will automatically apply the changes to all other nodes.

Figure 25: SCP policy version pane

Note: If Dell SCP policies have already been onboarded in Azure, you will see a "green" circular icon displayed next to the checkbox in the "Onboard Dell Server Configuration Profile Policies for Azure Arc" pane.

6 Remediate SCP policies

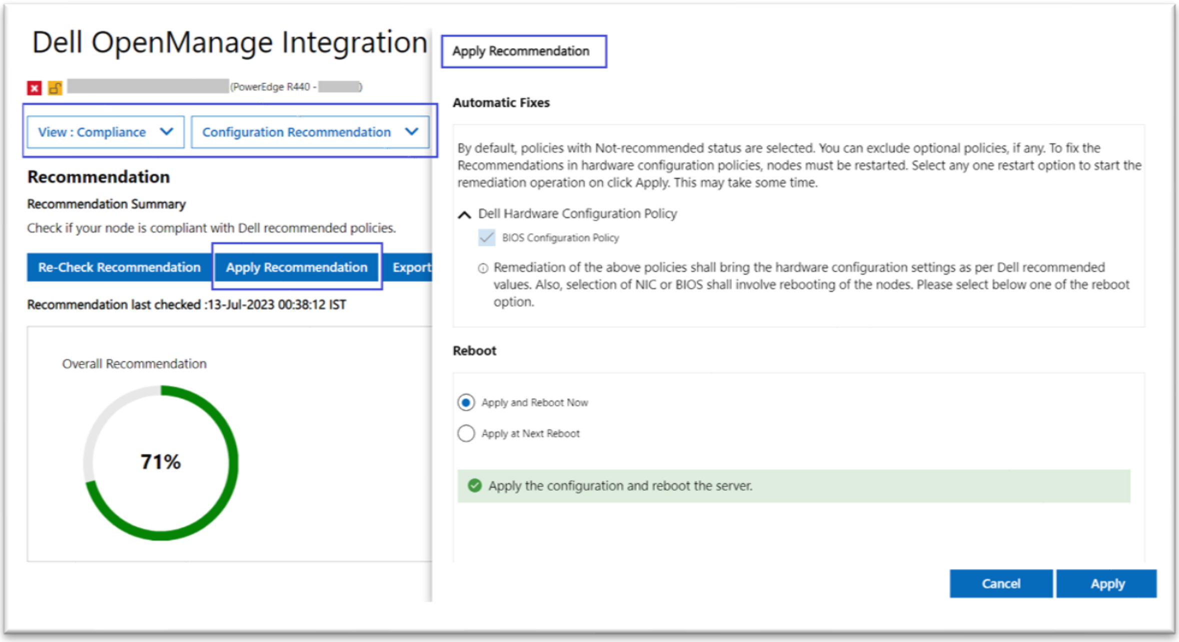
After you onboard the policies into Azure Arc (see Onboard policies into Azure), you can use OpenManage Integration with Windows Admin Center to manage Dell SCP policy compliance. This includes remediating Dell SCP policy to fix any non-compliant policies.


Dell OpenManage Integration
[redacted] (PowerEdge R440 - [redacted])
View : Compliance
Configuration Recommendation
Action
Recommendation
Recommendation Summary
Check Recommendation
Apply Recommendation
Export recommendation summary

Check if your node is compliant with Dell recommended policies.

Figure 26: Check Recommendation using Configure Recommendation

From the **View** drop-down, click **Compliance** and then from the next drop-down menu, click **Configuration Recommendation**. Next, click **Check Recommendation** to automatically compare the recommended rules packaged together in the Dell SCP policy definitions with the server configurations. These rules include configurations addressing the hardware, high-level compatibility, and security configurations.



Check if your node is compliant with Dell recommended policies.

Recommendation last checked :13-Jul-2023 00:38:12 IST

By default, policies with Not-recommended status are selected. You can exclude optional policies, if any. To fix the Recommendations in hardware configuration policies, nodes must be restarted. Select any one restart option to start the remediation operation on click Apply. This may take some time.

☑ BIOS Configuration Policy

Remediation of the above policies shall bring the hardware configuration settings as per Dell recommended values. Also, selection of NIC or BIOS shall involve rebooting of the nodes. Please select below one of the reboot option.

● Apply and Reboot Now

○ Apply at Next Reboot

✓ Apply the configuration and reboot the server.

Figure 27: Apply Recommendation

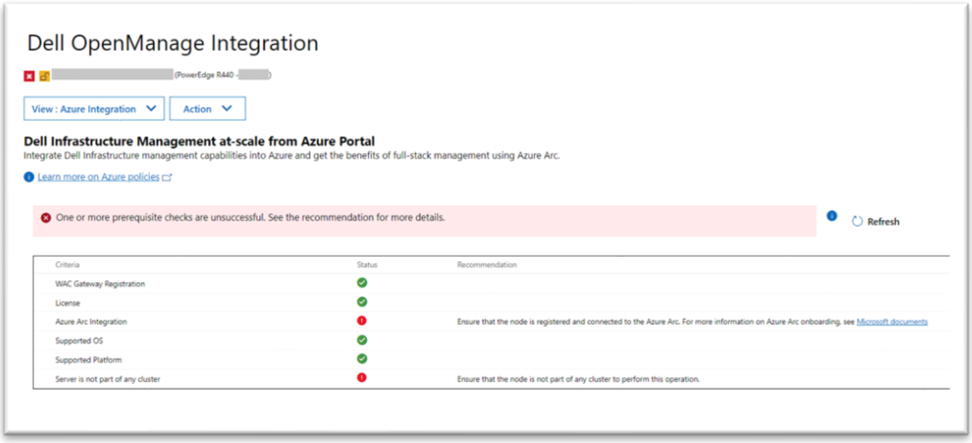
You can view the compliance report that is generated. If any server configurations are found to be non-compliant by Dell SCP Policies, you can then proceed to fix them using **Apply Recommendation**. On the **Apply Recommendation** pane, follow the recommendations to fix the compliance issues. Click **Apply** to resolve issues listed below **Automatic Fixes** for Dell Hardware Configuration Policy.

7 Troubleshooting

7.1 Prerequisite check failure

When you click **Azure Integration,** the extension checks if your server meets all the prerequisites that are mentioned in the “Prerequisite” section.

If any prerequisite checks fail, you are redirected to the **Prerequisite** page instead of the Azure Integration main page. You see an error banner message that displays showing the status and recommendations for the prerequisite checks. Follow the recommendations to resolve the prerequisite issues.



Dell OpenManage Integration

[redacted] (PowerEdge R440 - [redacted])

Dell Infrastructure Management at-scale from Azure Portal
Integrate Dell Infrastructure management capabilities into Azure and get the benefits of full-stack management using Azure Arc.

Learn more on Azure policies

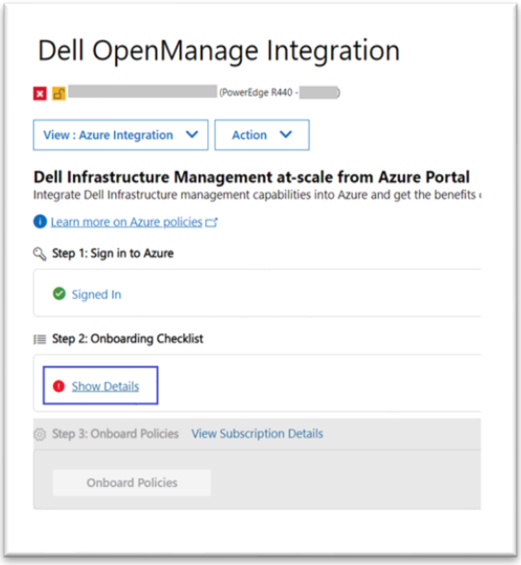
One or more prerequisite checks are unsuccessful. See the recommendation for more details.

Criteria	Status	Recommendation
WAC Gateway Registration	✓	
License	✓	
Azure Arc Integration	!	Ensure that the node is registered and connected to the Azure Arc. For more information on Azure Arc onboarding, see Microsoft documents
Supported OS	✓	
Supported Platform	✓	
Server is not part of any cluster	!	Ensure that the node is not part of any cluster to perform this operation.

Figure 28: Prerequisite check failure

7.2 Onboarding checklist failure

If any of the checklist requirements fail, see the recommendations on the **Onboarding Checklist** section for a fix. After the issue is fixed, click **Refresh** to get the latest status.



Dell OpenManage Integration

[redacted] (PowerEdge R440 - [redacted])

Dell Infrastructure Management at-scale from Azure Portal
Integrate Dell Infrastructure management capabilities into Azure and get the benefits

Learn more on Azure policies

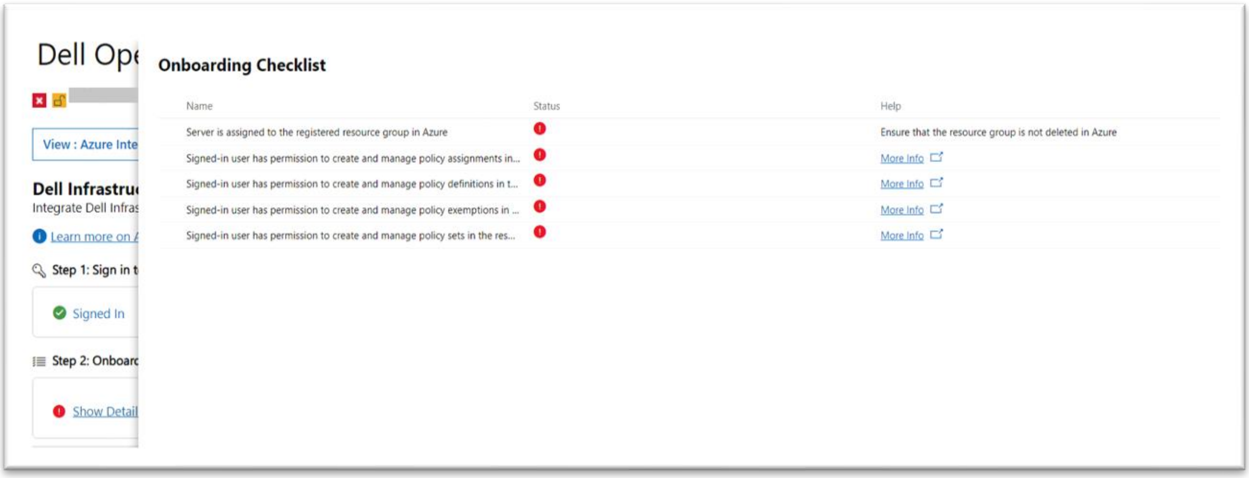
Step 1: Sign in to Azure

Signed In

Step 2: Onboarding Checklist

Step 3: Onboard Policies View Subscription Details

Figure 29: Onboarding checklist failure status



Onboarding Checklist

Name	Status	Help
Server is assigned to the registered resource group in Azure	●	Ensure that the resource group is not deleted in Azure
Signed-in user has permission to create and manage policy assignments in...	●	More Info
Signed-in user has permission to create and manage policy definitions in t...	●	More Info
Signed-in user has permission to create and manage policy exemptions in ...	●	More Info
Signed-in user has permission to create and manage policy sets in the res...	●	More Info

Figure 30: Onboarding checklist pop-up page – Failure Status

In case you encounter an onboarding checklist failure that is related to resource groups, refer to the Microsoft links provided in the Help column. For the first onboarding checklist item, follow these steps to address the issue:

- Verify that the resource group has not been deleted in the Azure. If it is deleted, create a resource group and assign the server to it. Then retry this operation from the beginning by navigating to the **Azure Integration** from the **View** menu.
- If the resource group is not deleted, rerun the **Step-2 Onboarding Checklist** step after a reasonable interval. Sometimes, the failure may be due to internal issues while fetching resource group information from Microsoft.

8 Conclusion

Using this white paper, one can easily use OMIMSWAC to onboard Dell SCP policies on Azure Arc for monitoring PowerEdge servers using Azure.

A. Technical Support and Resources

For more information about the user documentation, see the OpenManage Integration with Microsoft Windows Admin Center product support page at https://www.dell.com/support.

A.1 Related Resources

- OMIMSWAC's User's Guide, Release Notes, and Security Configuration Guide, see link.
- Microsoft Windows Admin Center Overview, see link.
- Connect hybrid machines to Azure from Windows Admin Center, see link.
- Connect hybrid machines to Azure using a deployment script, see link.
- Azure built-in roles, see link.
- Create and manage policies to enforce compliance, see link.
- Register Windows Admin Center with Azure, see link.