



Deploying Template and Configuring VLANs on Dell Networking IOAs with Dell OpenManage Essentials

A how to and best practices guide for using Dell OpenManage Essentials to deploy template and configure VLANs on Dell Networking IOAs.

Dell Engineering
July 2016

Revisions

Date	Description
September 2015	Initial release
July 2016	Added support for Dell Networking IOAs

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2016 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND

AT: <http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector> Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. QLogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.



Table of contents

Revisions	2
Executive Summary	6
1 Covered Features	7
2 Preparing OME for Device Configuration	8
2.1 Target device requirements	8
2.2 File share settings	8
2.2.1 File share requirement explanation	9
2.2.2 How to setup the file share	9
3 Understanding the differences between bare metal and stateless deployments	10
4 How to deploy in a stateless environment	11
5 How to replace a server in a stateless environment	12
6 How to reclaim virtual identities deployed by OME	13
7 How to deploy to a bare metal device	14
8 How to configure VLANs on server-facing ports of IOAs along with server deployment	15
9 How to automate hardware configuration and operating system deployment (Auto Deploy) of recently ordered devices	16
10 How to detect and manage configuration drift of a device in a production environment	17
11 Hardware setup for stateless environment	18
12 Create Templates	19
12.1 Template definition	19
12.2 Requirements for creating a template	19
12.3 How to create a template from a reference device	19
12.3.1 Create a template from a reference server	19
12.3.2 Create a template from a reference chassis	21
12.3.3 Create a template from a reference IOA	21
12.4 How to create a template from an XML, INI, or TXT configuration file	21
12.4.1 File requirements	21
12.4.2 Create a template from an XML file	21
12.4.3 Create a template from an INI file	22
12.4.4 Create a template from a TXT file	23
12.5 Edit IOA VLAN Attributes in Server Template	23



13	Create Virtual IO Pools.....	25
13.1	Virtual IO Pool definition	25
13.2	Types of identities	25
13.2.1	MAC Address Definition	25
13.2.2	World Wide Node Name (WWNN) Definition	26
13.2.3	World Wide Port Name (WWPN) Definition.....	26
13.2.4	IQN Definition	26
13.3	How to create a Virtual IO Pool	27
13.3.1	Create an identity type definition from an import file.....	27
13.4	How to increase the size of a Virtual IO Pool	28
13.4.1	Increase a prefix based identity type's size	28
13.4.2	Increase an import based identity type's size	28
13.5	How to lock or unlock a Virtual IO Pool	28
14	Create Compute Pool	29
14.1	Compute Pool Components	29
14.2	How to create a Compute Pool.....	29
14.3	How to add devices to a Compute pool.....	29
15	Deploy Compute Pools.....	30
15.1	Deploy requirements.....	30
15.2	How to deploy a Compute Pool.....	30
15.3	Compute Pool Locks	31
16	Deploy Template to Bare Metal Devices.....	32
16.1	Deploy requirements	32
16.2	Purpose and definition of the 'Repurpose and Bare Metal' device group	32
16.2.1	How to add devices to the 'Repurpose and Bare Metal' device group	32
16.2.2	How to add an IOA to the 'Repurpose and Bare Metal' device group	33
16.3	How to deploy a template.....	34
16.3.1	Deploy a template to servers	34
16.3.2	Deploy a template to chassis.....	35
16.3.3	Deploy a template on IOA.....	35
16.3.4	How to edit the device specific attributes of a deploy template task	36
17	Configure VLANs on the server-facing ports of IOAs during template deployment on a server	38



17.1	Deploy a template to servers along with VLAN configuration of associated IOA ports.....	38
17.2	How to edit the IOA VLAN attributes during server template deployment.....	39
18	Auto Deploy Templates	40
18.1	Auto deploy requirements.....	40
18.2	How to setup auto deploy of a template	40
18.2.1	Create a service tag CSV file	40
18.2.2	Setup stateless auto deploy of a template to server service tags.....	41
18.2.3	Setup bare metal auto deploy of a template to server service tags.....	42
18.2.4	Setup auto deploy of a template to chassis service tags	44
18.3	How to modify the auto deployment settings.....	44
19	Deploy Network ISO Image	45
19.1	Deploy network ISO image requirements	45
19.2	How to deploy network ISO image.....	45
20	Configuration Compliance.....	47
20.1	Configuration compliance requirements.....	47
20.2	How to setup and run the configuration inventory	47
20.2.1	Modify configuration inventory credentials and/or schedule.....	47
20.2.2	Run configuration inventory per target	49
20.3	How to associate devices to a template	49
20.4	How to view and leverage the compliance report	49
21	Troubleshooting	51
21.1	Troubleshooting the file share	51
21.2	Troubleshooting creating a template	53
21.3	Troubleshooting creating a virtual IO pool	54
21.4	Troubleshooting deploying a template.....	54
21.5	Troubleshooting auto deploying templates.....	55
21.6	Troubleshooting deploying a network ISO	56
21.7	Troubleshooting configuration compliance	56
A	Additional resources	57
B	Boot-from-SAN Considerations	58
	Boot-from-SAN Using iSCSI	58
	Boot-from-SAN Using FC/FCoE	60



Executive Summary

With OpenManage Essentials (OME) version 2.2, it is now possible to configure basic settings and VLANs on Dell Networking IOAs in a one-to-many fashion. This white paper introduces the new features that are available to manage and configure IOAs for various use cases.

This white paper also covers the stateless computing feature that was introduced in OME version 2.1. Stateless computing provides a powerful abstraction that allows workloads to seamlessly move from hardware to hardware and scale workloads. Maintaining a stateless environment and quickly responding to errors is difficult.

This white paper also covers the device configuration features that were introduced in OME version 2.0. The device configuration features (deploying bare metal devices, auto deploy, configuration compliance) have changed and are important to understand in order to compliment the stateless feature set. Best practices and troubleshooting for the stateless and bare metal deployment and configuration are also included.



1 Covered Features

This white paper covers the following topics and features.

- Full use case examples for using the device configuration features that are available in OpenManage Essentials.
- Requirements and setup for using the features.
- Create a template from a server, chassis, or IOA.
- Create a virtual IO pool.
- Create a compute pool.
- Deploy a compute pool.
- Deploy a template to a server, chassis, or IOA.
- Deploy VLANs on the server-facing ports of IOAs during template deployment on the server.
- Deploy a template to undiscovered devices by service tag ('Auto Deploy').
- Deploy an ISO image from your network to a server.
- Check the compliance of devices against a template.



2 Preparing OME for Device Configuration

Device prerequisites and file share settings are required to use the configuration and deployment features in OME. This section covers the device requirements, how to setup the file share settings and troubleshooting for the file share settings.

2.1 Target device requirements

Target Server requirements:

- For Dell's 12th generation PowerEdge servers, the minimum supported version of iDRAC is 1.57.57.
- For Dell's 13th generation PowerEdge servers, the minimum supported version of iDRAC is 2.0.
- 'Server configuration for OpenManage Essentials' license installed on the iDRAC. This is a separate license from the iDRAC license.
- iDRAC Enterprise or iDRAC Express license. This is a separate license from the 'Server configuration for OpenManage Essentials' license.

Target Chassis requirements:

- For the PowerEdge M1000e, the minimum supported version of CMC firmware for is 4.6.
- For the PowerEdge VRTX, the minimum supported version of CMC firmware is 1.3.

Target IOA requirements:

- Supported models:
 - PowerEdge M I/O Aggregator
 - PowerEdge FN410S
 - PowerEdge FN410T
 - PowerEdge FN2210S
- The minimum supported version of Dell Networking OS firmware is 9.10.
- Supported modes for bare-metal deployment:
 - Standalone
 - Programmable MUX (PMUX)
 - Virtual Link Trunk (VLT)
- Supported modes for VLAN configuration:
 - Standalone
 - Virtual Link Trunk (VLT)

2.2 File share settings

The device configuration and deployment features require a staging area (file share). This section explains the details of the file share and how to setup the file share.



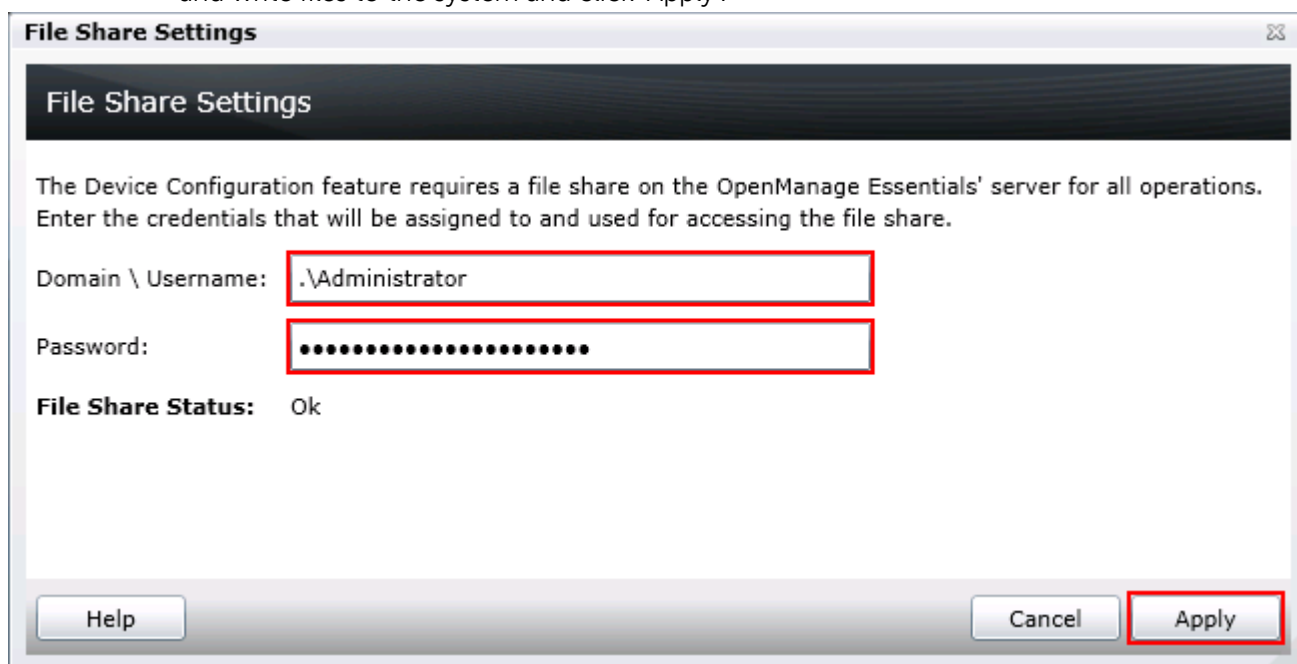
2.2.1 File share requirement explanation

The file share is a staging area for deployment. To use the deployment and configuration feature, a file share is required to send and receive configuration files to and from a device. During create or deploy task, configuration files will briefly exist in the file share folder. On completion of create or deploy task, the file is deleted. Security attributes (passwords and other sensitive data) are not included in the file.

2.2.2 How to setup the file share

The file share settings must be entered in OME. The file share settings require a username and a password. The username and password must be a user on the OME system that has enough privileges to read and write files on the system. During a deployment/configuration task, the username and password are sent to the remote targets to access the file share. Using an administrator account is recommended.

1. Navigate to the 'Deployment' portal.
2. Click 'File Share Settings' in the left hand navigation under the 'Common Tasks' section.
3. Enter the username and password of a user on the OME system that has enough privileges to read and write files to the system and click 'Apply'.



File Share Settings

The Device Configuration feature requires a file share on the OpenManage Essentials' server for all operations. Enter the credentials that will be assigned to and used for accessing the file share.

Domain \ Username: .\Administrator

Password:

File Share Status: Ok

Help Cancel Apply

Figure 1The file share settings popup

3 Understanding the differences between bare metal and stateless deployments

Bare metal and stateless are the two methods of deployment available from OME version 2.1 onwards. The primary differentiator between these is who controls the virtual identities assigned to the device.

In bare metal deployment, the user defines the identities and manually enters these into OME. This could also be considered manual identity deployment. The benefits of this is that the user can choose exactly which identity gets tied to each interface. The drawbacks are that the user must manually type this in and must also make sure not to reuse an identity on multiple interfaces. Also for this mode the use of compute pools is optional.

Stateless deployment allows the user to define a range of identities as a virtual IO pool and then OME will manage the assignment of the pool and automatically assign identities from the pool to devices. This expedites the deployment process and removes the burden from the user for ensuring an identity is not accidentally reused. Compute pools are required for this mode.



4 How to deploy in a stateless environment

Example use case – You want to deploy and manage servers in a virtualized environment connected to a storage area network. You want the configuration of one well formatted server deployed to other servers and you want the servers to use virtual identities created from manageable virtual identity definitions.

To accomplish this use case you must perform the following steps.

1. Get the configuration from the device that is already configured and save it in OME as a template. (See the [How to create a template from a reference device](#) section).
2. Create the definitions of the identities you wish to deploy. This is accomplished in OME by creating a "Virtual IO Pool". (See the [How to create a Virtual IO Pool](#) section).
3. Create a deployment definition that describes what to deploy and what servers to deploy against. This is accomplished in OME by creating a "Compute Pool". (See the [How to create a Compute Pool](#) section).
4. Deploy the compute pool deployment definition to the target devices. (See the [How to deploy a Compute Pool](#) section).

Note: Creating a template and deploying a template have requirements for the OME system and for the target devices.

To review the requirements for deploying a template, see the [Deploy requirements](#) section.



5 How to replace a server in a stateless environment

Example use case – A server in your stateless environment experienced a hardware failure. You need to transfer the workload of the failing server to a new server.

To accomplish this use case you must perform the following steps.

Prerequisites:

- The source device must have been deployed from OME from a compute pool using virtual IO.
- The target device must be in the same compute pool as the source.

Steps:

1. Add the target device to the 'Repurpose and Bare Metal' device group if not already. (See the [How to add devices to the 'Repurpose and Bare Metal' device group](#) section).
1. Add the target device to the compute pool of the source device if it is not already.
2. Complete the replace server wizard to initiate the replace server task.
3. Verify the task succeeded in the task execution history.

Note: The virtual identities of the source server are deployed to the target server during this operation. If OME is unable to connect to the source and physically remove the identities, it will lead to network conflicts later if it is reconnected to the network.

The wizard will not be accessible if the prerequisites are not met.



6 How to reclaim virtual identities deployed by OME

Example use case – A production server with a specific workload needs retired, and you wish to reclaim all the virtual identities so OME can reuse these later.

To accomplish this use case you must perform the following steps:

Prerequisites:

The source device must have been deployed from OME from a compute pool using virtual IO.

Steps:

1. Complete the reclaim identities wizard to begin the reclaim process.
2. Verify the task succeeded in the task execution history.

Note: It is possible to reclaim the identities for re-use in OME whether or not the device is still visible in OME. However, if the device was already deleted from OME, the reclaim operation will not be able to physically remove the identities from the device, and if it were to be reconnected to the network in that case, it could result in network conflicts if the identities have been re-used. The wizard will not be accessible if there are no deployed identities to reclaim.



7

How to deploy to a bare metal device

Example use case – Based on your data center’s needs, you configure all the settings of one server or chassis or IOA. You have a new bare metal device or device you want to repurpose. You wish to copy all of the settings of the configured device and apply them to bare metal/repurpose device.

To accomplish this use case you must perform the following steps.

1. Get the configuration from the device that is already configured and save it in OME as a template. (See the [How to create a template from a reference device](#) section).
2. Add the target device (the bare metal device) to the ‘Repurpose and Bare Metal’ device group. (See the [How to add devices to the ‘Repurpose and Bare Metal’ device group](#) section).
3. Deploy the template to the target device. (See the [How to deploy a template](#) section).

Note: Creating a template and deploying a template have requirements for the OME system and for the target devices.

To review the requirements for creating a template, see the [Requirements for creating a template](#) section.

To review the requirements for deploying a template, see the [Deploy requirements](#) section.



8 How to configure VLANs on server-facing ports of IOAs along with server deployment

Example use case – You are using VLAN tagging in your networking infrastructure to control packet flow. Additionally, you are using specific VLANs to control communication with modular servers enforced by chassis IOAs. Based on your data center's needs, you configure all the settings of one modular server. You have a new bare metal/repurpose modular server. You want to copy all of the settings of the configured modular server and apply them to a bare metal/repurpose modular server along with the VLANs that you want to configure on connected ports of chassis IOAs.

To accomplish this use case you must perform the following steps.

1. Get the configuration from the server that is already configured and save it in OME as a template. (See the [Create a template from a reference server](#) section).
2. Edit the template to assign tagged and untagged VLANs on each of the server-facing ports of IOAs. (See the [Edit IOA VLAN Attributes in Server Template](#) section).
3. Add the target server (the bare metal device) to the 'Repurpose and Bare Metal' device group. (See the [How to add devices to the 'Repurpose and Bare Metal' device group](#) section).
4. Deploy the template to the target server along with the VLAN configuration of the associated IOA ports. (See the [Configure VLANs on the server-facing ports of IOAs during template deployment on a](#) section).

Note: Creating a template and deploying a template have requirements for the OME system and for the target devices. Additionally, associated chassis IOAs must be discovered in OME and should meet minimum requirements for the VLAN configuration step to succeed. See the [Target device requirements](#) section.

To review the requirements for creating a template, see the [Requirements for creating a template](#) section.

To review the requirements for deploying a template, see the [Deploy requirements](#) section.



9 How to automate hardware configuration and operating system deployment (Auto Deploy) of recently ordered devices

Example use case - Your Company orders several new devices. The devices are shipped and may come in at different times. When a device is connected to the network, you want a template you created deployed to the device and for the devices to boot to an ISO on your network.

Note: Auto deploy is only for devices that have not been discovered by OME. To deploy to devices discovered by OME, see the [Deploy Template](#) section. Also, Dell Networking IOAs cannot be deployed using the Auto deploy feature.

To accomplish this use case you must perform the following steps.

1. Create a template from a configured device or sample template. (See the [How to create a template from a reference device](#) section).
2. Add deployment instructions for the devices (auto deploy entries) you want automatically configured after they are discovered. Devices are added by service tag. (See the [How to setup auto deploy of a template](#) section).
3. Discover the devices in OME when the devices are running and connected to the network.

Note: Creating a template and auto deploying a template has requirements for the OME system and for the target devices.

To review the requirements for creating a template, see the [Requirements for creating a template](#) section.

To review the requirements for auto deploying a template, see the [Auto deploy requirements](#) section.



10 How to detect and manage configuration drift of a device in a production environment

Example use case - You have deployed templates to several servers and chassis and want to verify that the attribute values of the template match the attribute values of the devices. If a device does drift from the template, you want to know which attributes are different.

Note: The device configuration compliance feature is not available for Dell Networking IOAs.

To accomplish this use case you must perform the following steps.

1. Get the configuration data from a device, import a template, or use an existing template for compliance. This template will be used to check configuration drift of target devices and will be referred to as a 'compliance template'. (See the [How to create a template from a reference device](#) section).
2. Set a schedule and credentials for getting the current configuration inventory from target devices. The process is called 'Configuration Inventory Schedule'. (See the [How to setup and run the configuration inventory](#) section).
3. Select a compliance template for the devices by associating the devices to a template. (See the [How to associate devices to a template](#) section).
4. Use the 'Configuration' portal to determine compliance and drift. (See the [How to view and leverage the compliance report](#) section).

Note: Creating a template and configuration compliance has requirements for the OME system and for the target devices.

To review the requirements for creating a template, see the [Requirements for creating a template](#) section.

To review the requirements for the configuration compliance, see the [Configuration compliance requirements](#) section.



11 Hardware setup for stateless environment

This section covers the hardware setup and best practices for configuring an environment for stateless computing.



12 Create Templates

Understanding and creating templates is necessary for using the deployment and configuration features. This section explains what a template is and how to create a template from a reference device or from a file.

12.1 Template definition

A template is a collection of attributes that describe the settings of a device. The settings describe the behavior of a device's hardware. A device may have several hundred attributes depending on the device's hardware. An attribute is a name value pair that describes a particular setting of a device. The configuration template of an IOA is a set of device properties and CLI commands in plain text format. OME installs with sample server and chassis templates for specific use cases. A user can deploy, edit, clone, delete, or rename a template. Sample templates must be cloned to deploy or use for compliance.

Note: Dell Networking IOA templates cannot be edited within OME. It is also recommended not to edit the IOA templates outside of OME. Deployment of edited IOA templates may fail because of various reasons.

12.2 Requirements for creating a template

To create a template from a reference device, the device must meet the same requirements in the [Target device requirements](#) section. To create a template, a server **does not** need a license.

12.3 How to create a template from a reference device

This section describes how to create a template from a discovered device. A 'reference device' is a device that has been discovered in OME, configured a desired way and the functionality of the device is intended to be replicated on other devices. The reference template is crucial to the success of configuring your other devices. Make sure that the reference device is correctly configured before you create a template from it.

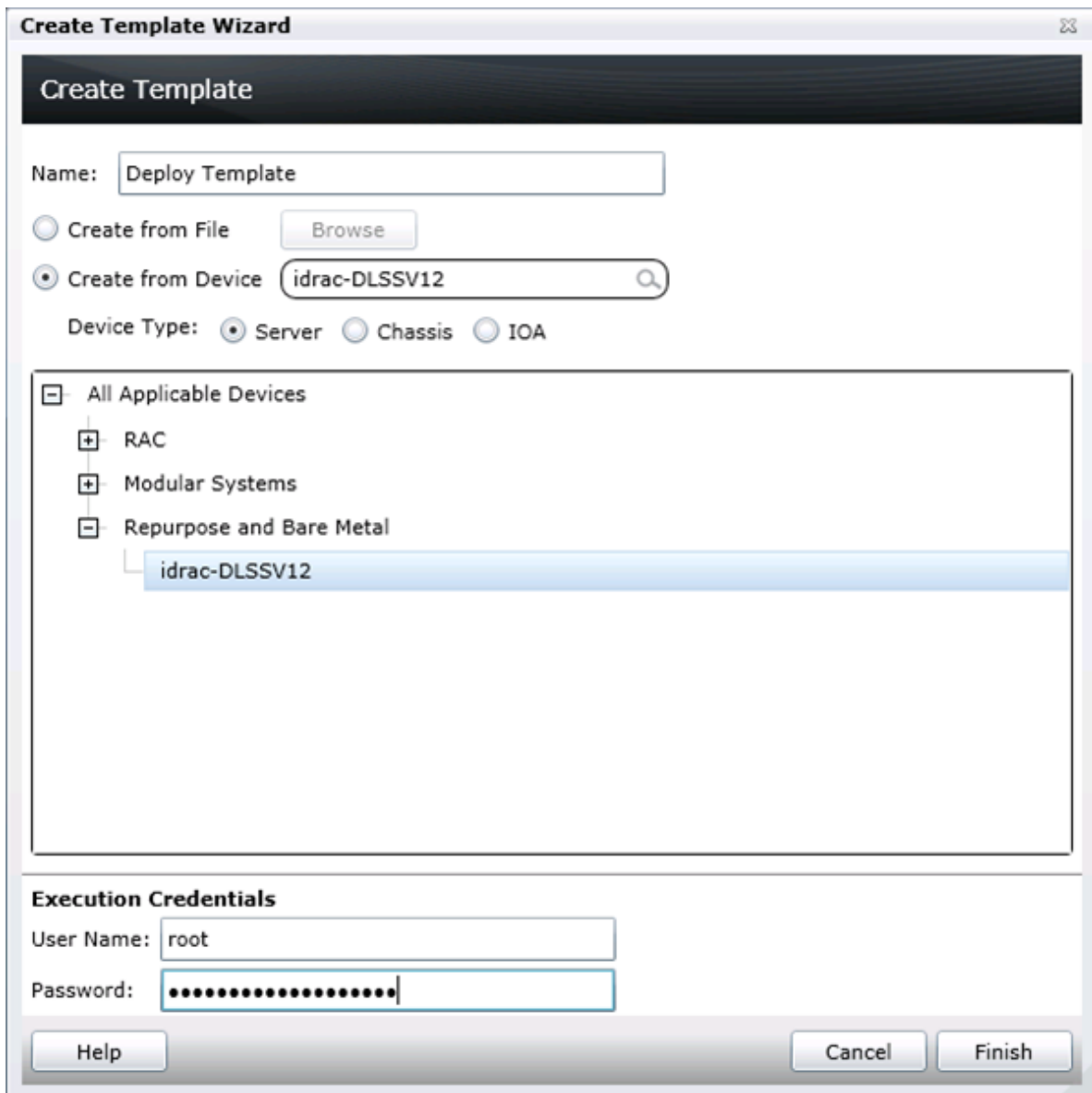
12.3.1 Create a template from a reference server

1. Navigate to the 'Deployment' tab.
2. Click 'Create Template' (located in the left hand navigation under 'Common Tasks').
3. Enter a unique name for the template.
4. Select 'Create from Device'.
5. Select the target server from the device tree

Note: Alternatively you can select the target by entering the device name or service tag in the search box next to the 'Create from Device' button.

6. Enter 'Execution credentials' for the target. The credentials must have administrator privileges on the target iDRAC.





Create Template Wizard

Create Template

Name:

☐ Create from File

☒ Create from Device

Device Type: ☒ Server ☐ Chassis ☐ IOA

☒ All Applicable Devices

- ☒ RAC
- ☒ Modular Systems
- ☒ Repurpose and Bare Metal
 - ☒ idrac-DLSSV12

Execution Credentials

User Name:

Password:

Figure 2 Create template from reference device wizard

7. Click 'Finish'.
8. Click 'OK' to the task created message.

A task is created when the wizard is closed. To view the created task, click the 'Tasks' tab in the 'Deployment' portal. To view the progress of the task, look at the 'Task Execution History' grid. To view the details of the execution history, double click the task execution history entry, or right click the task execution history entry and select 'Details'. The details will inform you if any problems occurred (such as incorrect credentials, etc.).

If the task is successful, a template is created and displayed in the 'Server Templates' tree.

If the task is not successful, view the details of the task by double clicking the execution history. The task can be run again by right clicking the task execution history or the task and clicking 'Run'. Rerunning the task requires entering the iDRAC credentials.

12.3.2 Create a template from a reference chassis

Follow the steps in the [Create a template from a reference server](#) section. After step 4, select 'Chassis' in the device type section. The execution credentials in step 6 must have administrator privileges on the CMC.

12.3.3 Create a template from a reference IOA

Follow the steps in the [Create a template from a reference server](#) section. After step 4, select 'IOA' in the device type section. The execution credentials in step 6 must have administrator privileges on the IOA.

12.4 How to create a template from an XML, INI, or TXT configuration file

The following section describes how to create a template from an XML, INI, or TXT configuration file. Configuration XML is used for server templates. The INI format is used for chassis templates. The TXT format is used for IOA templates. A configuration file can be obtained by exporting a template to file in OME. Configuration template files are also available from the Dell TechCenter.

12.4.1 File requirements

Files used for a template must meet the following requirements.

XML file:

- Must be well formed XML.
- Must contain at least one attribute.

INI file:

Must be well formed INI.

TXT file:

Must be a valid Dell Networking IOA configuration file.

12.4.2 Create a template from an XML file

1. Navigate to the 'Deployment' tab.
2. Click 'Create Template' (located in the left hand navigation under 'Common Tasks').
3. Enter a unique name for the template.
4. Select 'Create from File'.
5. Click the 'Browse' button and browse to the file's location.
6. Select the file and click 'Open'.



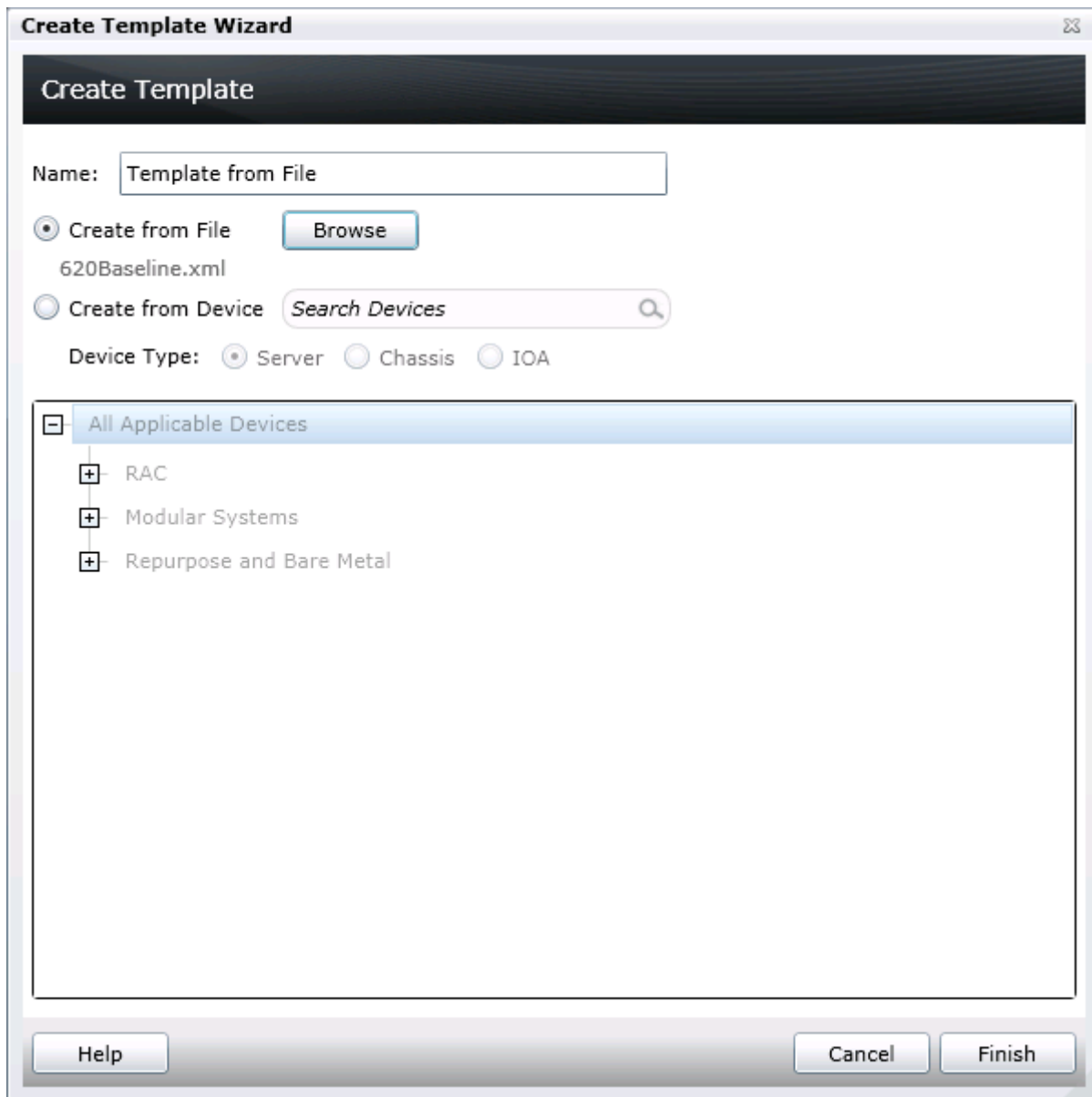


Figure 3 Create template from file wizard

7. Click Finish to create the template.
8. The template name will be added in the 'Server Templates' tree.

12.4.3 Create a template from an INI file

The INI format is for chassis devices and creating a template from an INI file will create a chassis template. Follow the same steps in the [Create a template from an XML file](#) section. In step 5, when browsing for the file's location, select the '.ini' file type option. The template will be added in the 'Chassis Templates' tree.

12.4.4 Create a template from a TXT file

The TXT format is for IOA devices and creating a template from a TXT file will create an IOA template. Follow the same steps in the [Create a template from an XML file](#) section. In step 5, when browsing for the file's location, select the '.txt' file type option. The template will be added in the 'IOA Templates' tree.

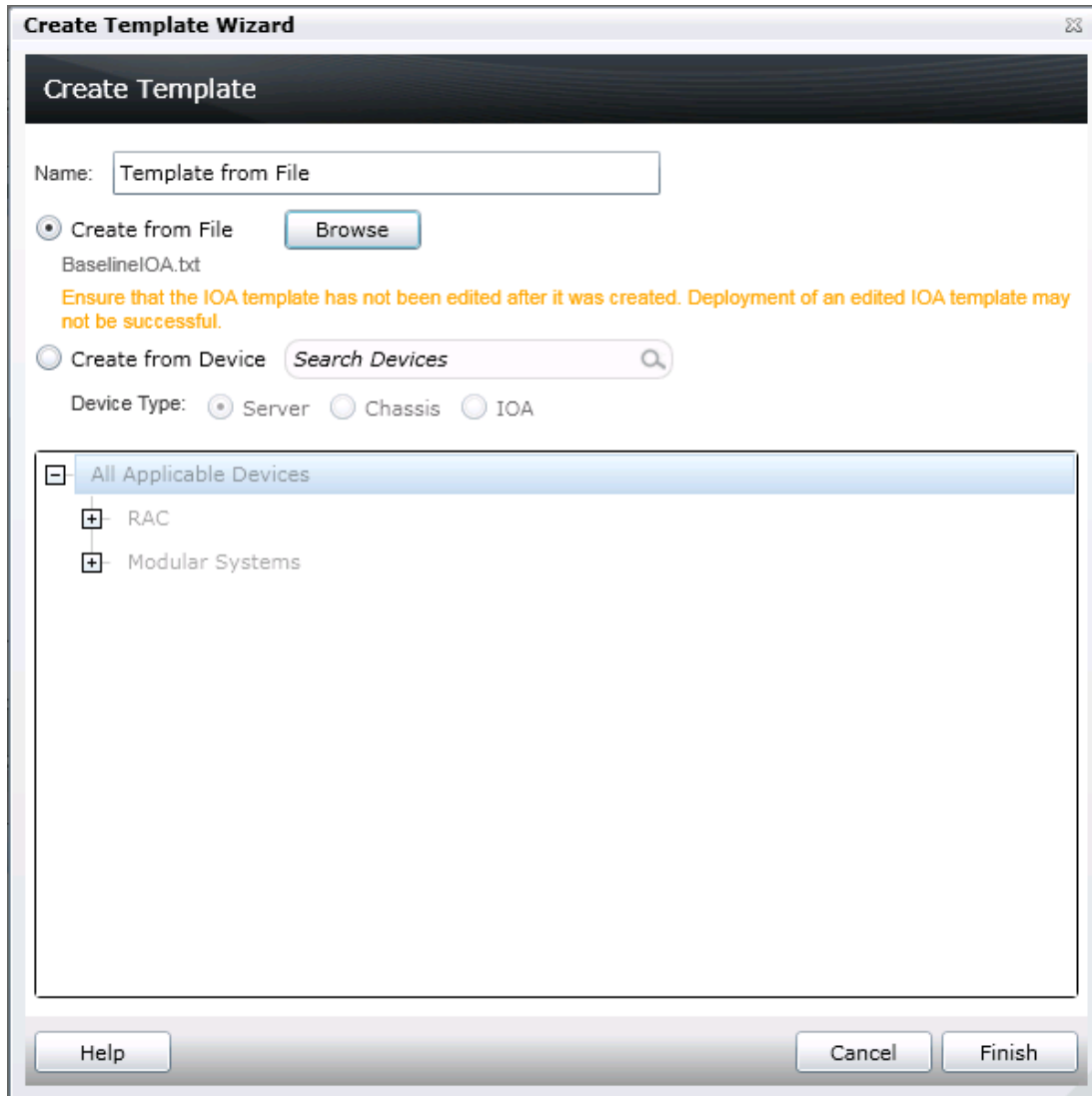


Figure 4 Create IOA template from TXT file

12.5 Edit IOA VLAN Attributes in Server Template

The following section describes how you can edit and assign IOA VLAN attributes for a particular template created from a modular server. This step enables VLAN assignment on the server-facing ports of IOAs during configuration template deployment on sever.



Note: IOA VLAN Attributes will only be available with templates created from modular servers.

1. Navigate to the 'Deployment' tab.
2. Select a template under 'Templates' → 'Server Templates' in the left-hand side navigation tree.
3. Select 'IOA VLAN Attributes' tab on right-hand side template details.
4. Assign the 'Tagged VLAN(s)' and 'Untagged VLAN' values for the ports that you want to configure.
5. Click 'Save' to save the changes to the template.

The screenshot displays the Dell OpenManage Essentials web interface. The top navigation bar includes 'Home', 'Manage', 'Deployment', 'Reports', 'Settings', 'Logs', 'Tutorials', and 'Dell Solutions'. A search bar on the right says 'Search device, ranges, and more...'. The left-hand navigation pane is expanded to show 'Deployment' and 'Templates'. Under 'Templates', 'Server Templates' is selected, and 'Server 1' is highlighted. The main content area shows the 'Server 1' configuration page with the 'IOA VLAN Attributes' tab selected. The page includes 'Undo' and 'Save' buttons. Below these is a table with columns: Deploy, Modified, NIC, Fabric, Tagged VLAN(s), and Untagged VLAN. The table contains four rows of data, with the second row highlighted. The status bar at the bottom of the table indicates 'Total: 4' and 'Modified: 2'.

Deploy	Modified	NIC	Fabric	Tagged VLAN(s)	Untagged VLAN
<input checked="" type="checkbox"/>	Yes	NIC.Integrated.1-3-1	A1	1-100	101
<input checked="" type="checkbox"/>	Yes	NIC.Integrated.1-4-1	A2	1-100	101
<input type="checkbox"/>	No	NIC.Integrated.1-1-1	A1		
<input type="checkbox"/>	No	NIC.Integrated.1-2-1	A2		

Figure 5 Edit IOA VLAN attributes

13 Create Virtual IO Pools

Virtual IO pools simplify identity management in OME. This section explains how to create a virtual IO pool from a prefix definition or from an import file. Also covered in this section is how to increase a virtual IO pool's size and lock or unlock a virtual IO pool.

13.1 Virtual IO Pool definition

A virtual IO pool is a definition of identity types that describe identities and determines the identities OME will generate. A virtual IO pool may contain identity definitions for different types of identities.

13.2 Types of identities

Virtual IO pools may contain different identity type definitions. Identity types define the identity properties required for a specific network protocol; for example an Ethernet MAC address.

An identity type is defined by specifying a prefix and the number of predefined octets (except for IQN which is defined by an IQN seed string) or by importing identities from a file. The number of predefined octets is how many octets are defined by the user. All generated identities of that identity type will begin with the prefix. Any remaining octets are used to generate addresses by OME. The number of predefined octets allows OME to know when to stop generating address so overlap does not occur. Imported identities must be unique and pass the restriction checks mentioned below. Imported identities are used as is by OME.

13.2.1 MAC Address Definition

MAC addresses are used for virtual MAC address properties. It is recommended to define this in all SAN types.

An example of MAC address is *00-14-22-01-23-45*. Please note that this will vary depending on the environment and vendor HBA cards.

Restrictions:

MAC address prefixes cannot be a multicast address. A multicast address is an address with a value of 1 in the least-significant bit of the first octet. (So 01, 03, 0B etc. are not allowed).

Defined by:

- Prefix address
- Number of predefined octets

Or

- Imported identities



13.2.2 World Wide Node Name (WWNN) Definition

WWNN addresses are used to define virtual WWNN address properties. It is recommended to define this in FCoE and FC environments only.

For example, 21:00:00:e0:8b:05:05:04 is the identity for QLogic HBA card. Please note that this will vary depending on the vendor HBA cards.

Restrictions:

WWN prefixes require an NAA value of 2, 5 or 6. An NAA value (Network Address Authority) is a 4 bit field used to guarantee uniqueness of WW names. The NAA value is the first four bits of the address (so the address must start with 2, 5 or 6).

Defined by:

- Prefix address
- Number of predefined octets

Or

- Imported identities

13.2.3 World Wide Port Name (WWPN) Definition

WWPN addresses are used to define virtual WWPN address properties. It is recommended to define this in FCoE and FC environments only.

Restrictions:

WWPN prefixes have the same NAA restrictions mentioned in the section above.

Defined by:

- Prefix address
- Number of predefined octets

Or

- Imported identities

13.2.4 IQN Definition

IQN addresses are used to define virtual IQN addresses. It is recommended to define this in iSCSI environments only.

An example for IQN is: *iqn.2001-09.com.example:mystorage.disk1.test1.abc*

Restrictions:

Value cannot be empty.

Defined by:

- IQN seed string

Or

- Imported identities

13.3 How to create a Virtual IO Pool

A virtual IO pool can be created from the deployment portal. A virtual IO pool may contain an identity definition for each of the types of identities. Multiple definitions for a single identity type is not allowed. A virtual IO pool may contain identity types defined by prefix and/or import files. To create a virtual IO pool follow the steps below:

1. Navigate to the 'Deployment' tab.
2. Click 'Create Virtual IO Pool' (located in the left hand navigation under 'Common Tasks').
3. Enter a unique name (and optionally a description) and click next.
4. Enter a MAC address prefix and click next.
5. Enter a WWNN address prefix if the stateless environment is FC or FCoE. Otherwise, uncheck the "Include Fibre Channel WWNN Identities in the Pool" checkbox. Click next.
6. Enter a WWPN address prefix if the stateless environment is FC or FCoE. Otherwise, uncheck the "Include Fibre Channel WWPN Identities in the Pool" checkbox. Click next.
7. Enter an iSCSI IQN string if the stateless environment is iSCSI. Otherwise, uncheck the "Include IQN Identities in the Pool" checkbox. Click next.
8. Review and click "Finish".

13.3.1 Create an identity type definition from an import file

An identity type may be defined using an import file. This section covers the file requirements and how to import the identities from a CSV file.

13.3.1.1 File Requirements

The imported file must meet the following requirements:

1. The file must have a CSV extension.
2. Identity types are limited to 10,000 imported identities. Any identity over this count will be discarded.
3. The CSV file must have a column title. The title may be any name.
4. Imported items must meet the requirements in the Types of identities section above.



13.3.1.2 Import identities from a CSV file

To import identities from a file, perform the steps below:

1. In the "Create Virtual IO Pool" in the identity type screen (example "Ethernet Identities" screen) check the "Import from file:" radio button.
2. Click the "Import" button.
3. An import wizard pops up. Click the "Import" button.
4. Select a file.
5. Wait for the import to finish (progress bar shows status).
6. Review results and close the results window.
7. (Optional) import additional files (repeat steps 3-6).
8. Click the "Close" button.

The imported identities may be viewed in this wizard by clicking the "View" button in the "Create Virtual IO Pool" wizard.

13.4 How to increase the size of a Virtual IO Pool

While assigning or deploying identities, a virtual IO pool may run out of identities. The number of identities in a virtual IO pool may be increased. This section covers how to increase the size of a virtual IO pool.

13.4.1 Increase a prefix based identity type's size

To increase the number of identities for an identity defined by a prefix, decrease the number of predefined octets. This can be done by editing the virtual IO pool and decreasing the number of predefined octets. This will remove octets defined by the user. It is suggested to move one octet at a time as decreasing one predefined octet greatly increases the number of identities OME can generate.

13.4.2 Increase an import based identity type's size

To increase the number of identities for an identity defined by an import file, import more identities via file. The import operation does not overwrite the previous identities and is an additive operation. To review how to import identities to a virtual IO pool see the [Import identities from a CSV file](#) section.

13.5 How to lock or unlock a Virtual IO Pool

A virtual IO pool's lock state is determined by the lock state of all the compute pools associated to a virtual IO pool. A locked virtual IO pool cannot change the identity type definitions or imported identities of the virtual IO pool. To unlock a virtual IO pool, unlock all locked compute pools associated to the virtual IO pool. The compute pool summary page is useful for sorting by virtual IO pool and the lock state. It is suggested to only perform this if you plan on redeploying to call devices in the previously locked compute pools.



14 Create Compute Pool

Compute pools provide a method to group a set of like devices for deployment and pre-configure the settings which will be applied to them. The pool can be recalled at deployment time, simplifying the deployment process.

Compute pools are required for virtual IO.

Compute pools are visible in the deployment portal and under the main device tree under the repurpose and bare metal group.

14.1 Compute Pool Components

The compute pool definition includes several optional components:

Template – the template will define the attributes which will be available to deploy. Once defined for a compute pool, the template cannot be reused for another compute pool.

Network ISO – defines the network iso to deploy for the compute pool

IO Assignment type

- User defined IO – the user will define the IO attributes manually, this will operate like bare metal deployment
- Automatic IO – OME will fill in the virtual identities for selected attributes and manage the identities

Devices – defines the devices that are part of the pool. Note a device can be a member of only 1 pool.

14.2 How to create a Compute Pool

Launch and complete the create compute pool wizard to create the pool. The compute pool should be immediately visible in the compute pool navigation after the wizard is completed.

Note – this action only defines the pool in OME. It has not yet created any task or applied any setting to any device. You must next deploy the compute pool to apply this definition.

Note – many of the steps in the wizard are optional at creation time, however required components will be enforced before a deployment is possible.

14.3 How to add devices to a Compute pool

You can add devices to a compute pool at any time (even when locked), by doing a right-click edit of the compute pool and you can still add or remove devices from the pool.

15 Deploy Compute Pools

Deploying the compute pool is required to actually apply the settings in the pool definition to one or more devices in the pool.

15.1 Deploy requirements

1. The file share must be configured (see the [How to setup the file share](#) section).
2. The target devices must meet the minimum requirements for the deployment and configuration features (see the [Target device requirements](#) section).
3. The target devices must be added to the Repurpose and Bare Metal device group (see the [How to add devices to the 'Repurpose and Bare Metal' device group](#) section).
4. At least one user created template (a cloned sample template is a user created template).
5. The compute pool must have been created already using the create compute pool action.

See the [deploy template for bare metal](#) section for more background on general deployment requirements.

15.2 How to deploy a Compute Pool

Right click -> deploy on a compute pool to launch the deploy template wizard for the pool and deploy it.

1. Ensure the compute pool is selected as the deploy target.
2. The template defined by the pool should be pre-selected.
3. The IO assignment for the pool should be pre-selected. Note for stateless management, the setting should be on automatic IO assignment with a virtual IO pool selected.
4. Select the devices you wish to deploy. This will be limited to devices already included in the pool definition.
5. You can optionally edit attributes. If you have already defined the attribute settings during pool creation, then this will not be needed.
6. You can optionally assign identities and view them. This option is available on the identity attributes tab available only when virtual IO is being used. This action will reserve identities even if the wizard is later cancelled. If you do not need to see the identities before deployment, this step can be skipped as the task will automatically do the assignment if identities are not already reserved.



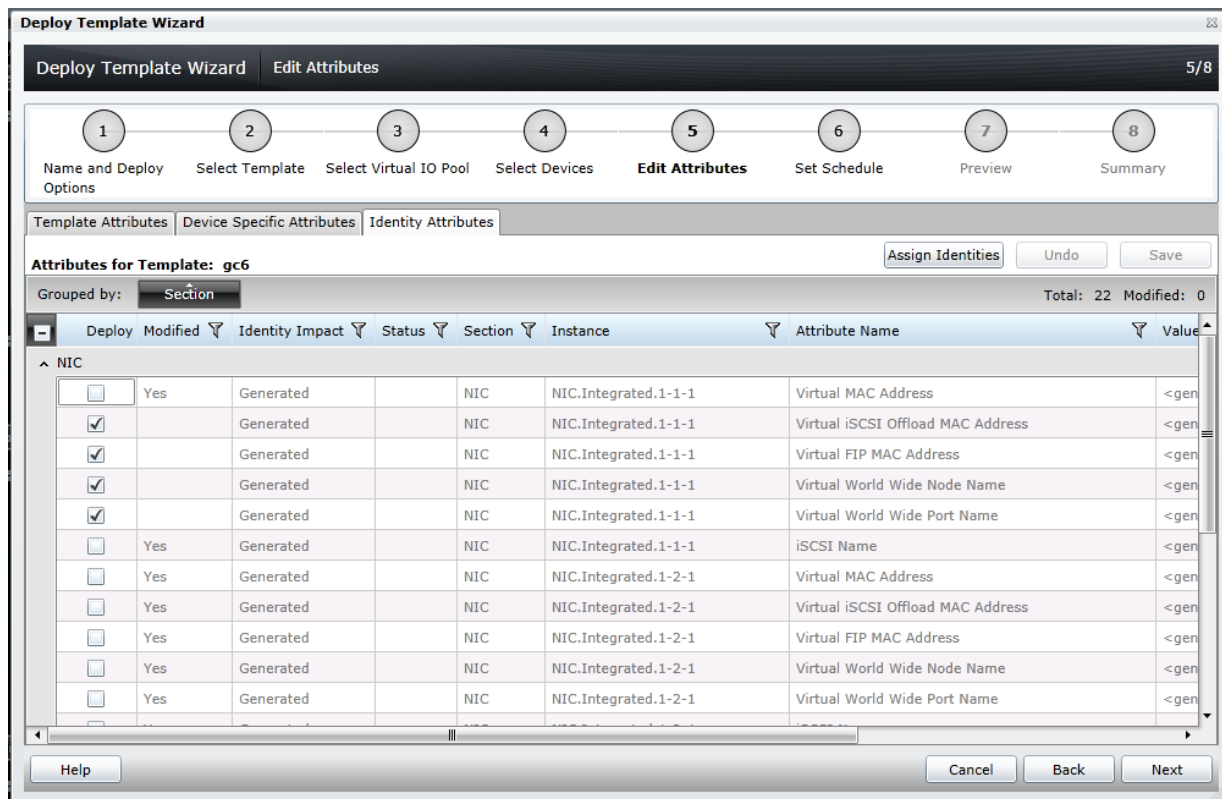


Figure 6 Assign identity attributes

7. Define the task start time.
8. You can optionally preview the task results. This will simulate the deploy action and show the results of what would occur when the task is run.
9. Completing the wizard will create and schedule the task for execution.
10. You should verify the task result by reviewing the task execution history for the task after it runs.

15.3 Compute Pool Locks

After successful deployment, the pool will become locked preventing the pool definition from being edited. The lock will affect the pool definition itself, the pool template, and the linked IO pool.

The purpose of the lock is to ensure the pool definition is not unintentionally altered after it has active deployments.

Note – you can still add and remove devices from the pool when it is locked.

It is possible to unlock the pool (right click action) which will also unlock the template and IO pool and re-enable editing.

16 Deploy Template to Bare Metal Devices

This section covers how to do deployment using manual IO which was introduced in OME 2.0. For stateless deployment, see the section [How to deploy a compute pool](#), and its prerequisite sections.

Deploying templates is the process of sending and applying configuration settings to remote devices. A template may contain a single configuration setting, configuration settings for one or more specific functional areas, or a full device configuration. To deploy a template, you must first create a template. The template is crucial to the success of the deploy task. Make sure the device you are creating the template from is configured exactly how you wish to deploy it when you create the template. To create a template, see the [Create Templates](#) section.

A template that was created from a target may contain destructive attributes (especially if it contains RAID configuration settings). Deploying destructive attributes may cause data loss, connectivity issues, failure to boot and other problems. It is important to review and understand each destructive attribute before deploying it to target devices.

16.1 Deploy requirements

1. The file share must be configured (see the [How to setup the file share](#) section).
2. The target devices must meet the minimum requirements for the deployment and configuration features (see the [Target device requirements](#) section).
3. The target devices must be added to the Repurpose and Bare Metal device group (see the [How to add devices to the 'Repurpose and Bare Metal' device group](#) section).
4. At least one user created template (a cloned sample template is a user created template).

16.2 Purpose and definition of the 'Repurpose and Bare Metal' device group

The Repurpose and Bare Metal device group is a device group containing all the devices eligible for the deploy template task. Only add devices to this group if you intend to deploy a template or an ISO image to the devices. If you do not intend to deploy a template or an ISO image to the devices, it is recommended that you remove the devices from the Repurpose and Bare Metal device group. You should not add production devices to the Repurpose and Bare Metal device group because deploying a template can be destructive and cause downtime or a loss of data.

16.2.1 How to add devices to the 'Repurpose and Bare Metal' device group

1. Navigate to the 'Deployment' tab.
2. Click 'Deployment Portal' in the left hand navigation under the 'Deploy Device Configuration Portal' heading.
3. Click the 'Repurpose and Bare Metal Devices' tab in the upper left area of the deployment portal.
4. Click the 'Modify Devices' button in the bottom right corner of the grid.
5. Check the target devices in the popup. The target devices must be discovered and any target server must have a 'Server configuration for OpenManage Essentials' license.



Note: Only devices that satisfy the deploy requirements appear in the device selection. To review the requirements, see the Deploy requirements section.

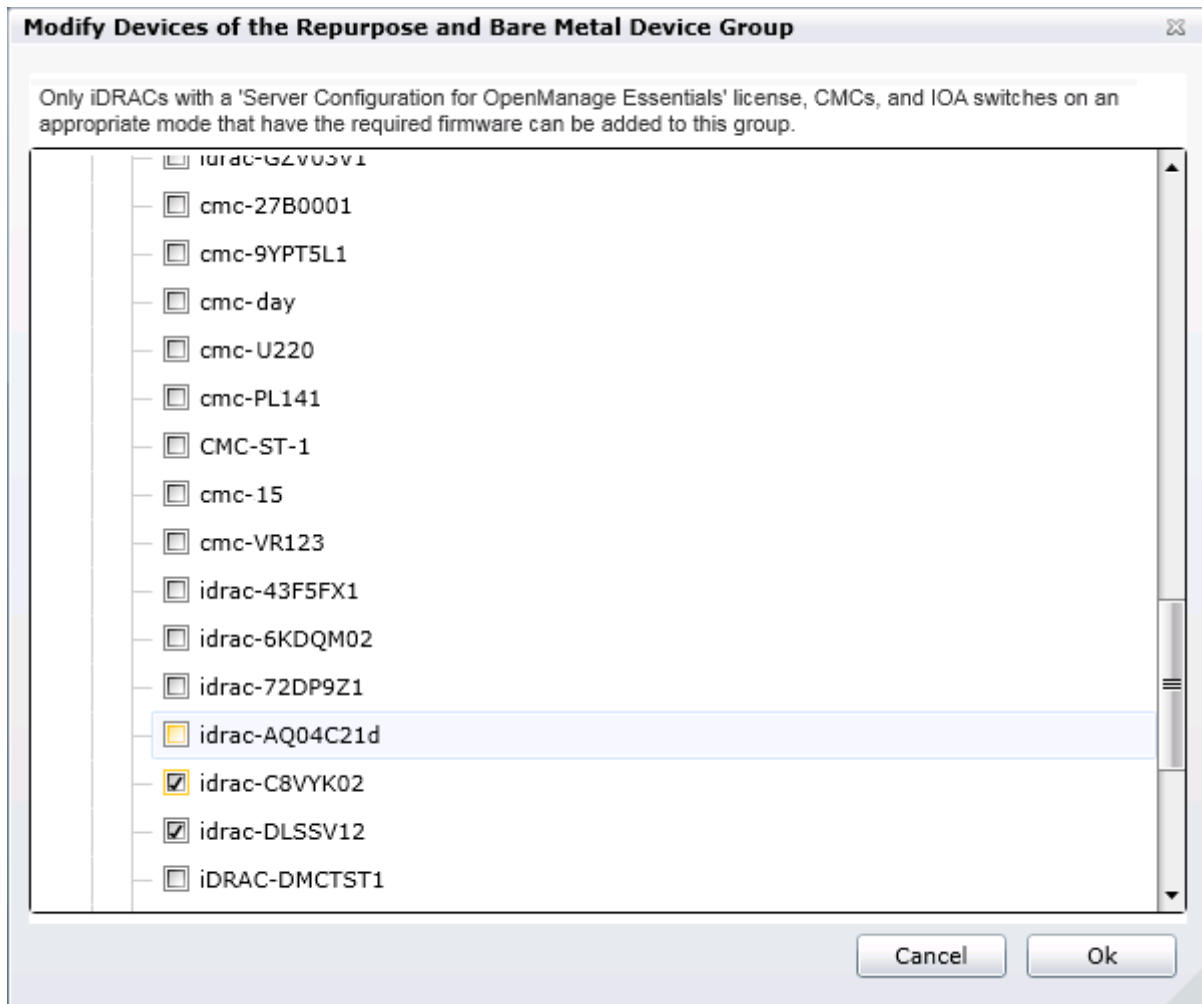


Figure 7 Modify repurpose and bare metal device group popup

6. Click 'Ok'.

16.2.2 How to add an IOA to the 'Repurpose and Bare Metal' device group

1. Navigate to the 'Deployment' tab.
2. Click 'Deployment Portal' in the left-hand navigation under the 'Deploy Device Configuration Portal' heading.
3. Click 'Modify Devices' button on the right-hand side corner of the grid.
4. Select the IOA devices under the Dell Networking Switches group. The IOA devices must be discovered and should be running in one of the supported modes.

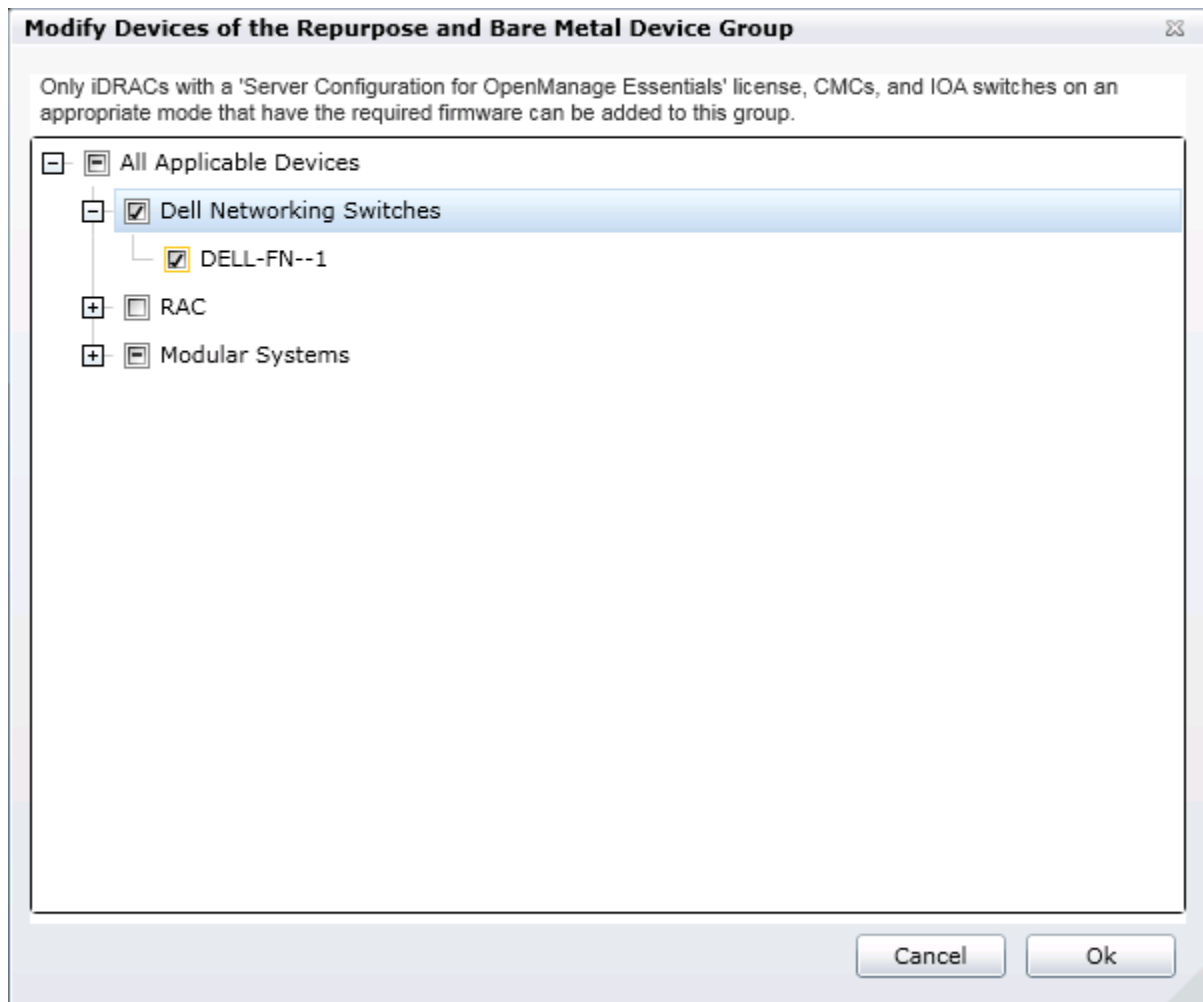


Figure 8 Adding IOA Devices to Repurpose and Bare Metal Group

5. Click 'Ok'.

16.3 How to deploy a template

This section describes how to deploy a template to servers, chassis and IOAs.

16.3.1 Deploy a template to servers

1. Navigate to the 'Deployment' tab.
2. Click 'Deploy Template' (located in the left hand navigation under 'Common Tasks').
3. Enter a unique name for the task. A name is optional since a default name is supplied, but it is a generic name, and the same default name is always supplied. Selecting a name that is relevant to what is being deployed is suggested.
4. Make sure 'Deploy Template' is selected and click 'Next'.
5. Select the template to be deployed on the target server/iDRAC and click 'Next'.

6. Select the target devices and click 'Next'.

Note: Only devices in the 'Repurpose and Bare Metal' device group and match the device type of the selected template (Server or Chassis) may be selected. See the [How to add devices to the 'Repurpose and Bare Metal' device group](#) section to add devices to the device group.

7. Enter the system specific attributes for each target device. These are attributes, such as 'Gateway IP Address', that are not included in templates because they do not necessarily apply to all target devices. For more details, see the [How to edit the device specific attributes of a deploy template task](#) section. Click 'Next'.
8. Set the schedule of when the deploy template task will run. 'Run now' will run the task when the wizard is closed. 'Run at' will run the task on the selected future date. Enter the credentials for all target devices. The credentials must be valid for all target devices and must have Operator or Administrator privileges on the iDRAC. Click 'Next'.
9. Review the task in the Summary pane and click 'Finish'.
10. Review the warning message. The deploy action can be destructive. It is important you review and understand the template you are deploying.

16.3.2 Deploy a template to chassis

A chassis template can be deployed to an unlicensed chassis. Follow the same steps in the [Deploy a template to servers](#) section. In step 5, select a Chassis template. In step 8, use credentials that have administrative privileges on the target CMCs.

16.3.3 Deploy a template on IOA

1. Navigate to the 'Deployment' tab.
2. Click 'Deploy Template' (located in the left-hand navigation under 'Common Tasks').
3. Enter a unique name for the task. A name is optional since a default name is supplied, but it is a generic name, and the same default name is always supplied. Selecting a name that is relevant to what is being deployed is suggested.
4. Make sure 'Deploy Template' is selected and click 'Next'.
5. Select the template under IOA Templates category to be deployed on the target IOA and click 'Next'.
6. Select the IOA device listed under the Dell Networking Switches group and click 'Next'.
7. Enter the system-specific attributes for each target device. The attribute, 'IOA host name', is not part of the templates because it does not necessarily apply to all target devices. For more details, see the [How to edit the device specific attributes of a deploy template task](#) section. Click 'Next'.
8. Following options are available for IOA templates deployment:
 - a. Perform pre-check only: To only verify (not deploy) if the device configuration template will be deployed successfully. If this option is selected, the 'Continue on warnings' option will be disabled.
 - b. Continue on warnings: To continue deploying the template even if the template is incompatible with the target device. When this option is selected, warnings (if any) will be ignored and the deployment task will continue to run.



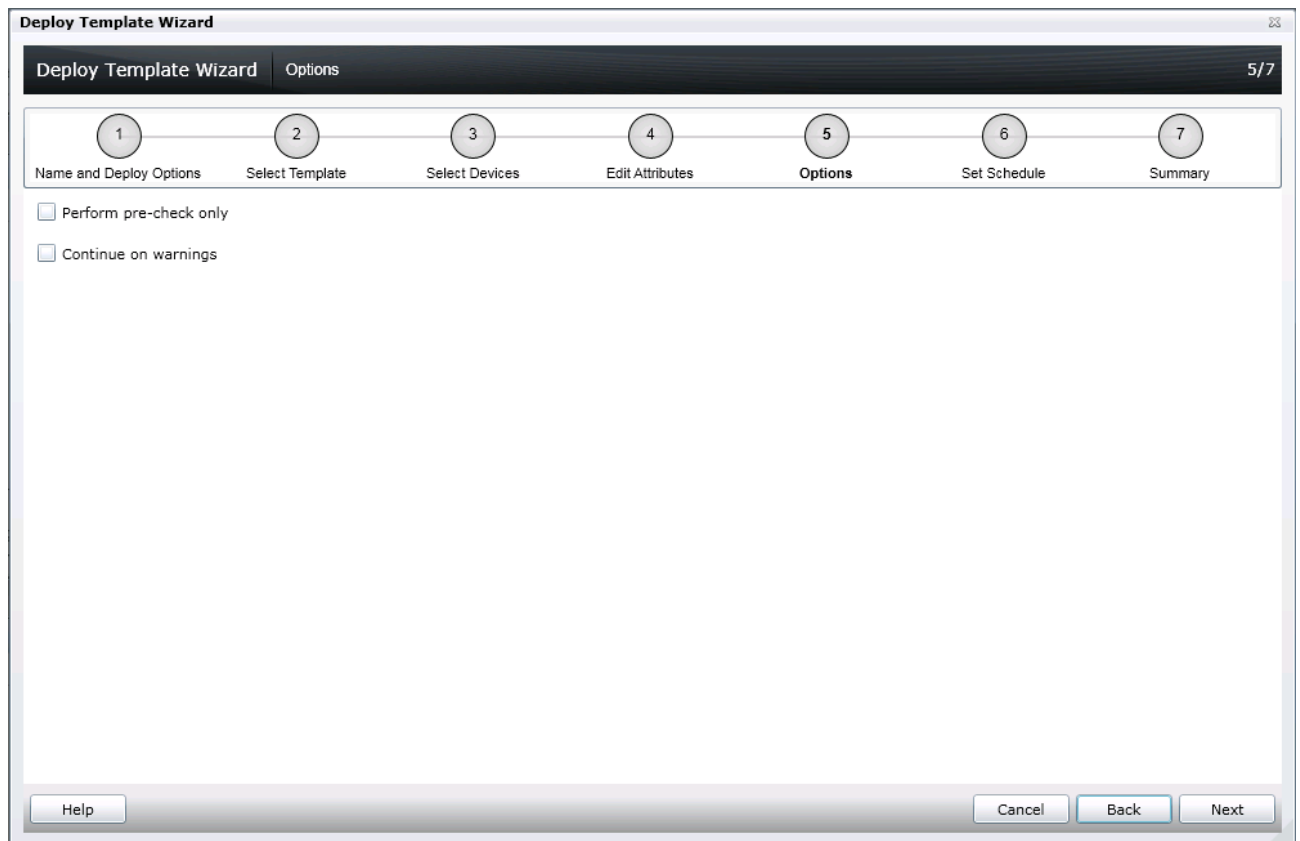


Figure 9 Selecting deploy options for IOA devices

9. Set the schedule of when the deploy template task will run. 'Run now' will run the task when the wizard is closed. 'Run at' will run the task on the selected future date. Enter the credentials for all target devices. The credentials must be valid for all target devices and must have Operator or Administrator privileges on the IOA. Click 'Next'.
10. Review the task in the Summary pane and click 'Finish'.
11. Review the warning message. The deploy action can be destructive. It is important you review and understand the template you are deploying.

16.3.4 How to edit the device specific attributes of a deploy template task

Device specific attributes are attributes, such as 'Gateway IP Address', that are not included in templates because they do not necessarily apply to all target devices. Editing and deploying device specific attributes is optional because a device may already have the device specific attributes configured or the attributes may not be applicable to that specific device. If the template being deployed has device specific attributes, the device specific attributes will appear in the 'Edit Attributes' page of the deploy wizard. The 'Edit Attributes' page lists the target devices on the left hand side and displays the device specific attributes for the selected device in the right hand side grid. To edit the attributes follow the steps below.

1. Select a device in the left hand tab.
2. Check 'Deploy' on the attributes that you want to deploy to that device.

3. Edit the 'Value' of each checked attribute. For more information, navigate to the Dell Attribute Registry site from the [Additional resources](#) section.
4. Click 'Save'.

Deploy Template Wizard

Deploy Template

1 Name and Deploy Options 2 Select Template 3 Select Devices **4 Edit Attributes** 5 Set Schedule 6 Summary

Template Attributes **Device Specific Attributes**

Select Devices: idrac-DMCTST1, **idrac-GJBBDV1**, idrac-GZV03V1

Device Specific Attributes for: idrac-GJBBDV1 [GJBBDV1, PowerEdge R720] Undo **Save** Import/Export

Grouped by: **Section** Total: 5 Modified: 2

Deploy	Modified	Section	Instance	Attribute Name	Value	Dependencies
System						
<input type="checkbox"/>		System	System.Embedded.1	ServerTopology 1 Data Center Name		
<input checked="" type="checkbox"/>	Yes	System	System.Embedded.1	ServerTopology 1 Aisle Name	Aisle_1	
<input type="checkbox"/>		System	System.Embedded.1	ServerTopology 1 Rack Name		
<input checked="" type="checkbox"/>	Yes	System	System.Embedded.1	ServerTopology 1 Rack Slot	7	
<input type="checkbox"/>		System	System.Embedded.1	ServerTopology 1 Room Name		

Help Cancel Back Next

Figure 10 Edit attributes pane

5. Repeat for each device.

Alternatively, you can import and export the grid to file to edit. You may want to export/import if you have a large number of devices with a large number of device specific attributes. The device specific attributes grid can be exported by selected device or all devices. All devices will export to a single file that can be opened in a spreadsheet processing application. When edits are finished in the file, the file may be imported. The edited values must be valid values for the attribute (see the attribute registry link in the [Additional resources](#) section). The grids will be populated with the import data. The UI logs will report any problems with format or values of the import file.

17 Configure VLANs on the server-facing ports of IOAs during template deployment on a server

This section describes how to configure VLANs on the server-facing ports of IOAs during template deployment on target servers.

17.1 Deploy a template to servers along with VLAN configuration of associated IOA ports

1. Navigate to the 'Deployment' tab.
2. Click 'Deploy Template' (located in the left-hand navigation under 'Common Tasks').
3. Enter a unique name for the task. A name is optional since a default name is supplied, but it is a generic name, and the same default name is always supplied. Selecting a name that is relevant to what is being deployed is suggested.
4. Make sure 'Deploy Template' is selected and click 'Next'.
5. Select the template to be deployed on the target server/iDRAC and click 'Next'.
6. Select the target devices and click 'Next'.

Note: Only devices in the 'Repurpose and Bare Metal' device group and match the device type of the selected template (Server or Chassis or IOA) may be selected. See [How to add devices to the 'Repurpose and Bare Metal' device group](#) section to add devices to the device group.

7. Click the IOA VLAN Attributes tab to edit the IOA VLAN attributes for the selected template. For more details, see the [How to edit the IOA VLAN attributes during server template deployment](#) section.

Note: IOA VLAN attributes are applicable to templates created from modular servers only. For selected modular servers during server template deployment, the VLANs will also be configured on the IOA ports facing the server NIC ports.

8. Enter the system-specific attributes for each target device. These are attributes, such as 'Gateway IP Address', that are not included in templates because they do not necessarily apply to all target devices. For more details, see the [How to edit the device specific attributes of a deploy template task](#) section. Click 'Next'.
9. Set the schedule of when the deploy template task will run. 'Run now' will run the task when the wizard is closed. 'Run at' will run the task on the selected future date. Enter the credentials for all target devices. Enter 'IOA Credentials' if deployable IOA VLAN attributes are present. The credentials must be valid for all target devices and must have Operator or Administrator privileges on the iDRAC. Click 'Next'.

Note: Fields to enter the 'IOA Credentials' will be displayed in the compute pool and auto-deploy deployment workflows as well if deployable IOA VLAN attributes are present with the template.

10. Review the task in the Summary pane and click 'Finish'.



- Review the warning message. The deploy action can be destructive. It is important you review and understand the template you are deploying.

17.2 How to edit the IOA VLAN attributes during server template deployment

During template creation from a modular server, IOA VLAN attributes are automatically added and linked to the server template. Once configured, these attributes are used to configure VLANs on the IOA ports that are facing the server NIC ports. If the template being deployed has IOA VLAN attributes, those will appear in the 'Edit Attributes' page of the deploy wizard. The 'Edit Attributes' page has 'IOA VLAN Attributes' tab that lists all available attributes for the selected template. To edit the IOA VLAN attributes, follow the steps below:

- Select 'IOA VLAN Attributes' tab on 'Edit Attributes' page.
- Select 'Deploy' on the attributes that you want to deploy.
- Provide the value for 'Tagged VLAN(s)' and 'Untagged VLAN'.
- Click 'Save'.

Deploy Template Wizard Edit Attributes 5/8

1 Name and Deploy Options 2 Select Template 3 Select Virtual IO Pool 4 Select Devices 5 **Edit Attributes** 6 Set Schedule 7 Preview 8 Summary

Template Attributes IOA VLAN Attributes Device Specific Attributes

IOA VLAN Attributes for Template: Server 1 Undo Save

Drag a column header and drop it here to group by that column Total: 4 Modified: 2

Deploy	Modified	NIC	Fabric	Tagged VLAN(s)	Untagged VLAN
<input checked="" type="checkbox"/>	Yes	NIC.Integrated.1-3-1	A1	1-100	101
<input checked="" type="checkbox"/>	Yes	NIC.Integrated.1-4-1	A2	1-100	101
<input type="checkbox"/>	No	NIC.Integrated.1-1-1	A1		
<input type="checkbox"/>	No	NIC.Integrated.1-2-1	A2		

Help Cancel Back Next

Figure 11 Edit IOA VLAN attributes

18 Auto Deploy Templates

Auto deploying templates applies all the template's attribute's values to a device after it has been discovered. To add auto deploy entries for devices that have not been discovered by OME, a list of service tags for the target devices must be provided. To auto deploy a template, you must first create a template. For instructions to create a template, see the [Create Templates](#) section.

Note: Auto deploy is only for devices that have not been discovered by OME. To deploy to devices discovered by OME, see the [Create Templates](#) section. Also, Dell Networking IOAs cannot be deployed using this feature.

18.1 Auto deploy requirements

In order to add auto deployment entries, the following requirements must be met:

1. Must have a template to deploy (see the [How to create a template from a reference device](#) section).
2. Must meet all device configuration target device requirements (see the [Target device requirements](#) section).
3. Target service tags cannot match a service tag of a discovered device.
4. A CSV file with the service tags (see the [Create a service tag CSV](#) section).

18.2 How to setup auto deploy of a template

This section describes how to setup auto deployment of a template against service tags. This section will cover the creation and format of the auto deployment CSV file and the auto deployment wizard.

18.2.1 Create a service tag CSV file

1. Create a csv file containing the target service tags to be deployed against. Follow the format below.
 - a. Must have a column named 'ServiceTag'.
 - b. Each service tag must match Dell standards for service tags.
 - c. Service tags may not match the service tag of a discovered device in OME.

	A
1	ServiceTag
2	ABCDEFGG
3	HY3912B
4	A123456
5	VNX189W

Figure 12 Format of an example CSV file.



18.2.2 Setup stateless auto deploy of a template to server service tags

1. Navigate to the 'Deployment' tab.
2. Click 'Setup Auto Deployment' (located in the left hand navigation under 'Common Tasks').
3. Select the target compute pool and click next.
4. Review the selected template and click next.
5. Review the selected virtual IO pool and click next.
6. Click the 'Import' button to import the csv file that contains the service tag or node ID. The imported service tags/node IDs must be compatible with the type of template selected in the step above.
7. Browse to the location where the file is saved, select the file and click Open. All the Service Tags in the file will be imported and listed in OME. The 'Import Summary' window is displayed. Review and click OK to close the window. Click 'Next'.
8. (optional) Enter the unique attributes per service tag (for more details, see the [How to edit the device specific attributes of a deploy template task](#) section). Note that virtual identities may be reviewed, but may not be assigned. Assignment occurs when the device is discovered. Click 'Next'.
9. Select the execution credentials for the service tags. Instead of entering the credentials for each target device, credential definitions must be created. Credential definitions can be added as needed. Credential definitions can be assigned to multiple targets. Credentials are required for each target device.
 - a. If no credentials exists yet, at least one (a default set of credentials) must be created. Follow these steps, otherwise go to step 9.
 - b. Click 'Add New Credential'.
 - c. Enter a description for the credential set (the description text is displayed in the credential selection page).
 - d. Enter the username and password.
 - e. Click 'Finish'.
10. Review the task in the Summary pane and click 'Finish'.
11. All the service tags/node IDs that were imported are listed in the 'Auto Deployment' tab.
12. The service tags remain in the 'Auto Deployment' tab until they are discovered and inventoried in OME and the 'Deploy Configuration to Undiscovered Devices' task creates a deploy task for the device with the service tag. The 'Deploy Configuration to Undiscovered Devices' task checks periodically if the devices are discovered and inventoried in OME. Once the discovery and inventory is complete and a deploy task is created, the devices will move to the compute pool and the auto deployment entry will be deleted. Deploy configuration tasks are created to deploy the templates that were selected. The tasks created for the service tag entries can be found under the tasks tab in the deployment portal. Double click on the task to view the task details. Task execution history entries can be found in the task execution history grid. Double click on a task execution history entry to view the task execution history details.



18.2.3 Setup bare metal auto deploy of a template to server service tags

1. Navigate to the 'Deployment' tab.
2. Click 'Setup Auto Deployment' (located in the left hand navigation under 'Common Tasks').
3. Make sure 'Deploy Template' is checked and click 'Next'.
4. Select a server or chassis template (as applicable to the type of target devices) to be deployed on the target servers or chassis and click 'Next'.
5. Click the 'Import' button to import the csv file that contains the Service Tags. The imported service tags must be compatible with the type of template selected in the step above.
6. Browse to the location where the file is saved, select the file and click Open. All the Service Tags in the file will be imported and listed in OME. The 'Import Summary' window is displayed. Review and click OK to close the window. Click 'Next'.
7. (optional) Enter the unique attributes per service tag (for more details, see the [How to edit the device specific attributes of a deploy template task](#) section) and click 'Next'.
8. Select the execution credentials for the service tags. Instead of entering the credentials for each target device, credential definitions must be created. Credential definitions can be added as needed. Credential definitions can be assigned to multiple targets. Credentials are required for each target device.
 - a. If no credentials exists yet, at least one (a default set of credentials) must be created. Follow these steps, otherwise go to step 9.
 - b. Click 'Add New Credential'.
 - c. Enter a description for the credential set (the description text is displayed in the credential selection page).
 - d. Enter the username and password.



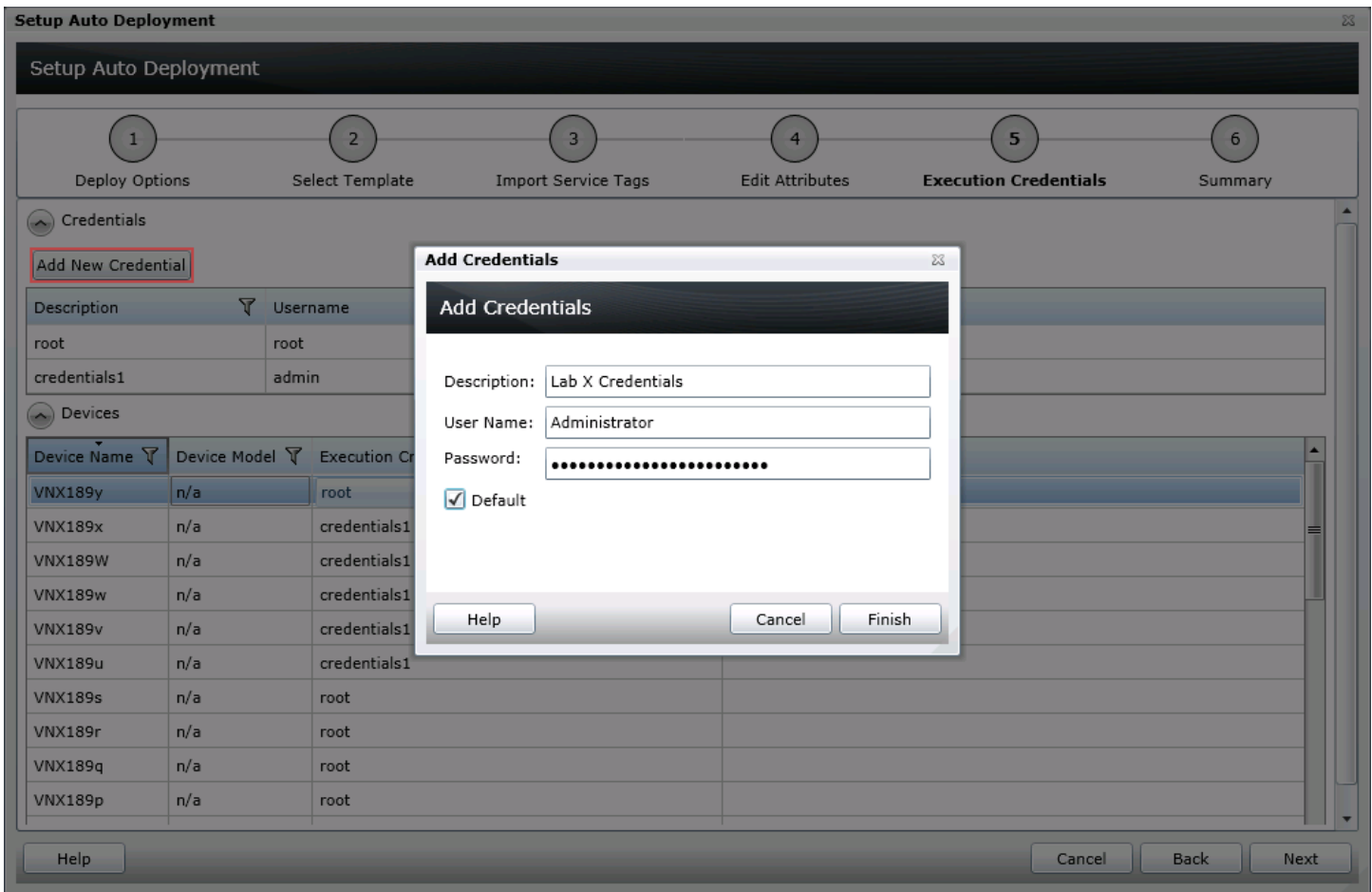


Figure 13 Auto deployment target credentials page

- e. Click 'Finish'.
9. Review the task in the Summary pane and click 'Finish'.
10. All the service tags that were imported are listed in the 'Auto Deployment' tab.
11. The service tags remain in the 'Auto Deployment' tab until they are discovered and inventoried in OME and the 'Deploy Configuration to Undiscovered Devices' task creates a deploy task for the device with the service tag. The 'Deploy Configuration to Undiscovered Devices' task checks periodically if the devices are discovered and inventoried in OME. Once the discovery and inventory is complete and a deploy task is created, the devices will move to the Bare Metal/Repurpose Devices group and the auto deployment entry will be deleted. Deploy configuration tasks are created to deploy the templates that were selected. The tasks created for the service tag entries can be found under the tasks tab in the deployment portal. Double click on the task to view the task details. Task execution history entries can be found in the task execution history grid. Double click on a task execution history entry to view the task execution history details.

18.2.4 Setup auto deploy of a template to chassis service tags

A chassis template can be deployed to an unlicensed chassis. Follow the same steps in the [Setup bare metal auto deploy of a template to server service tags](#) section. Select a service tag CSV file of chassis in step 6.

18.2.5 How to modify the auto deployment settings

By default, the 'Deploy Configuration to Undiscovered Devices' task runs every 60 minutes. When this task runs, it checks if any of the auto deployment service tags were discovered. If the device matching an auto deployment service tag was discovered, a deploy template task is automatically created and the specified template is deployed to that device. To modify the execution interval for the 'Deploy Configuration to Undiscovered Devices' task or to enable/disable it, follow the steps below.

1. Navigate to the 'Deployment Settings' tab under the 'Preferences' tab.
2. Check or uncheck the 'Enable auto deployment for recently discovered devices' to enable or disable the 'Deploy Configuration to Undiscovered Devices' task.

Note: If the task is disabled, the service tags in the 'Auto Deployment' grid will not be deployed to automatically.

3. Adjust the interval using the numeric control. The number is the minute interval that the 'Deploy Configuration to Undiscovered Devices' task will run.

The screenshot shows the 'Deployment Settings' page in the Dell OpenManage Essentials interface. The 'Auto Deployment Settings' section is highlighted with a red box. It contains a checked checkbox for 'Enable auto deployment for recently discovered devices' and a numeric control for 'Run auto deployment every 60 Minutes'. The 'File Share Settings' section above it shows fields for 'Domain \ Username' (set to '.\Administrator') and 'Password' (masked with dots). The 'File Share Status' is 'Ok'. At the bottom of the 'Auto Deployment Settings' section are 'Cancel' and 'Apply' buttons.

Figure 14 Auto deployment settings page

4. Click 'Apply'.

19 Deploy Network ISO Image

Deploying of a network ISO boots a server to an ISO image that is located on your network. This can be done independent, or in conjunction with a deployment task.

19.1 Deploy network ISO image requirements

- Must meet all Deploy Template requirements (see the [Target device requirements](#) section).
- If the 'Deploy Template' deploy option is checked, only server templates may be selected.

19.2 How to deploy network ISO image

1. Navigate to the 'Deployment' tab.
2. Click 'Deploy Template' (located in the left hand navigation under 'Common Tasks').
3. Enter a unique name for the task. A name is optional since a default name is supplied, but it is a generic name, and the same default name is always supplied. Selecting a name that is relevant to what is being deployed is suggested.
4. Check 'Boot to Network ISO' and uncheck 'Deploy Template'. Click 'Next'.

Note: Both 'Deploy Template' and 'Boot to Network ISO' can be selected. If both are selected, the 'Select Template' and 'Edit Attributes' tabs are added to the wizard. See the [Deploy a template to servers](#) section for a 'How to' on the 'Select Template' ([above](#)) and 'Edit Attributes' ([above](#)) tabs.

5. Enter ISO filename, Share IP, Share Name, Share username and Share password. Click 'Next'.



Deploy Template Wizard

Deploy Template

1 Name and Deploy Options 2 Select Template **3 Select ISO Location** 4 Select Devices 5 Edit Attributes 6 Set Schedule 7 Summary

ISO Filename
ISO Filename:

Share Location
Share IP:
Share Name:

Share Credentials
Share Username:
Share Password:

Figure 15 Select ISO location page

Note: The user must have full control to the share folder where the ISO is located. The share folder should be different than the file share used for deployment.

6. Select the target devices and click 'Next'.

Note: Only devices in the 'Repurpose and Bare Metal' device group may be selected. See the [How to add devices to the 'Repurpose and Bare Metal' device group](#) section to add devices to the device group.

7. Set the schedule of when the deploy template task will run. 'Run now' will run the task when the wizard is closed. 'Run at' will run the task on the selected future date. Enter the credentials for all target devices. The credentials must be valid for all target devices and must have Operator or Administrator privileges on the iDRAC. Click 'Next'.
8. Review the task in the Summary pane and click 'Finish'.

20 Configuration Compliance

Configuration compliance detects drift of a device's attributes from a template's attributes. A process called 'configuration inventory' gets configuration information (inventory) from all applicable devices and compares the inventory against an associated compliance template.

Note: Device configuration compliance feature is not available for Dell Networking IOAs.

20.1 Configuration compliance requirements

1. The file share must be configured (see the [How to setup the file share](#) section).
2. The target devices must meet the minimum requirements for the deployment and configuration features (see the [Target device requirements](#) section).
3. At least one user created template (a cloned sample template is a user created template).
4. Configuration Inventory must be enabled and the target device credentials must be provided.

20.2 How to setup and run the configuration inventory

The configuration inventory task collects the attribute information from all eligible devices. An eligible device is any device that meets the device configuration target requirements (see the [Target device requirements](#) section). The inventoried values are used to calculate the compliance of a device against the device's associated template.

Note: Dell Networking IOAs will not be listed for scheduled configuration inventory collection.

20.2.1 Modify configuration inventory credentials and/or schedule

The configuration inventory schedule and credentials may be modified. The configuration inventory can be turned off if network or performance problems are encountered. The steps below describe how to modify the schedule and set the credentials for the configuration inventory.

1. Navigate to the 'Configuration' tab under the 'Manage' tab.
2. Click on 'Configuration Inventory Schedule' in the left hand navigation under 'Common Tasks'.
3. If credentials have not been added, click on the 'Add New Credential'.
 - a. Enter a unique description name.
 - b. Enter the username and password that the target devices will use.
 - c. Select 'Default' for a credential to have discovered devices automatically assigned to the credential. One set of credentials must be assigned as the default.
4. Select the credentials for each device. Each device can have its own set of credentials. Click 'Next'.



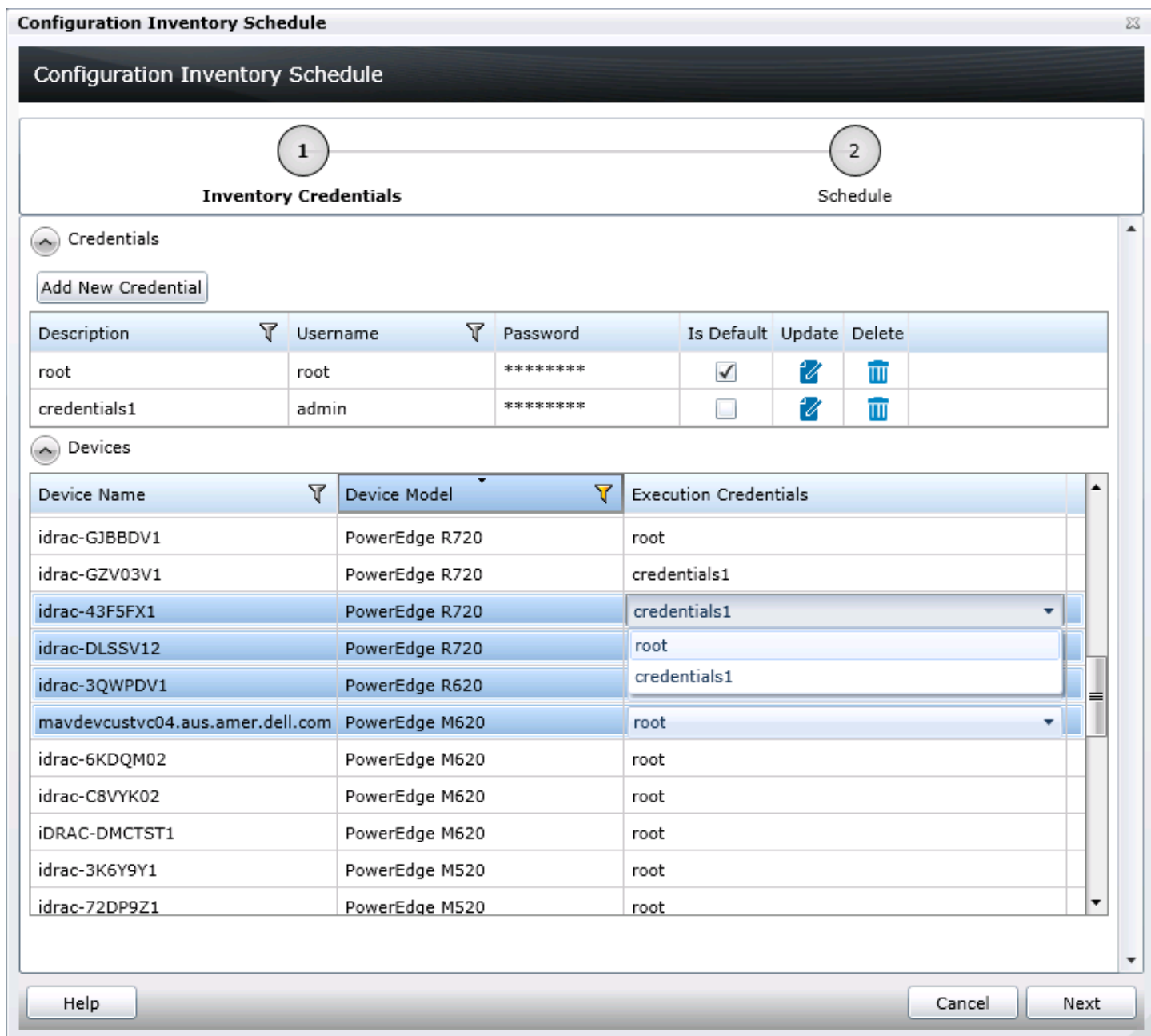


Figure 16 Configuration inventory credentials page

20.2.2 Run configuration inventory per target

To get the current configuration inventory from a device, do the following...

1. Navigate to the device tree ('Manage' -> 'Devices').
2. Select target devices and right click.
3. Hover over 'Device Configuration'.
4. Select 'Refresh Device Configuration Inventory'.

20.3 How to associate devices to a template

A device needs an associated compliance template for the device to have a compliance status in the compliance pie chart.

Note: Compliance does not include the device-specific attributes of a template. The IOA VLAN attributes, if available with the template, are also not included for compliance.

To set a compliance template for a device, you must associate the device to a template. A device may only have one associated template. To associate a device to a template, do the following...

1. Navigate to the 'Configuration' tab under the 'Manage' tab.
2. Click on 'Associate Devices to a template' in the left hand navigation under the 'Common Tasks' section.
3. Select a template and click 'Next'.
4. Select devices and click 'Finish'.

Note: Only devices that meet the device configuration requirements (see the [Target device requirements](#) section) and are of the same device type as the template are shown.

20.4 How to view and leverage the compliance report

The device compliance panel shows the configuration compliance status and state of all eligible devices (an eligible device is a device that meets the requirements in the [Target device requirements](#) section). Every eligible device is in one of the states below. Clicking a slice of the pie chart will show all the devices that have the selected pie slice's state. Device configuration compliance can be viewed in the 'Configuration' tab under the 'Manage' tab. The summary and pie chart have the following states. Actions required for the state are listed under each of the states below.

1. Compliant Devices
 - a. No action required.
2. Not Compliant Devices
 - a. Double click the compliance row to view differences between the associated template and the device's inventory.
 - b. Adjust the device's settings or associate to a different template to make the device compliant.
3. Not Inventoried Devices
 - a. Inventory the device. See the [How to setup and run the configuration inventory](#) section.



- b. Make sure the credentials for the target are accurate.
- 4. Not Associated Devices
 - a. Associate the devices to a template. See the [How to associate devices to a template](#) section.
- 5. Not Licensed Devices
 - a. Import a 'Server configuration for OpenManage Essentials' license in the device's iDRAC license interface.



21 Troubleshooting

21.1 Troubleshooting the file share

1. Check the file share status in OME.
 - a. The file share status is at the bottom of the file share wizard and is in the 'Deployment Settings' preference.

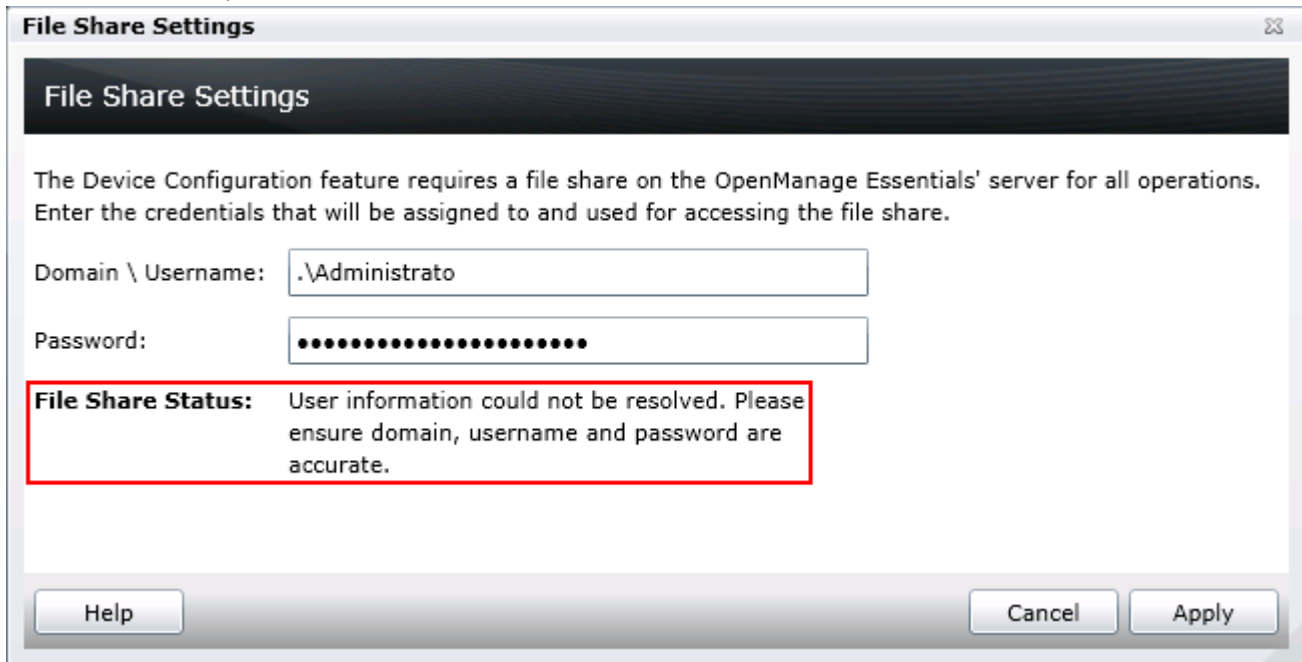


Figure 17 File share settings popup status

2. Check the username, domain and password in OME.
3. Check the share folder in Windows Explorer.
 - a. Verify the 'ServerConfig' folder exists under the installation configuration folder (by default under 'Program Files\Dell\SysMgt\Essentials\configuration').
 - b. Verify the folder is shared. Right click the folder, select 'Properties', select the 'Sharing' tab. The folder should be shared. The 'Advanced Sharing' permission settings should have the user entered in OME as the only user with permissions to the folder.

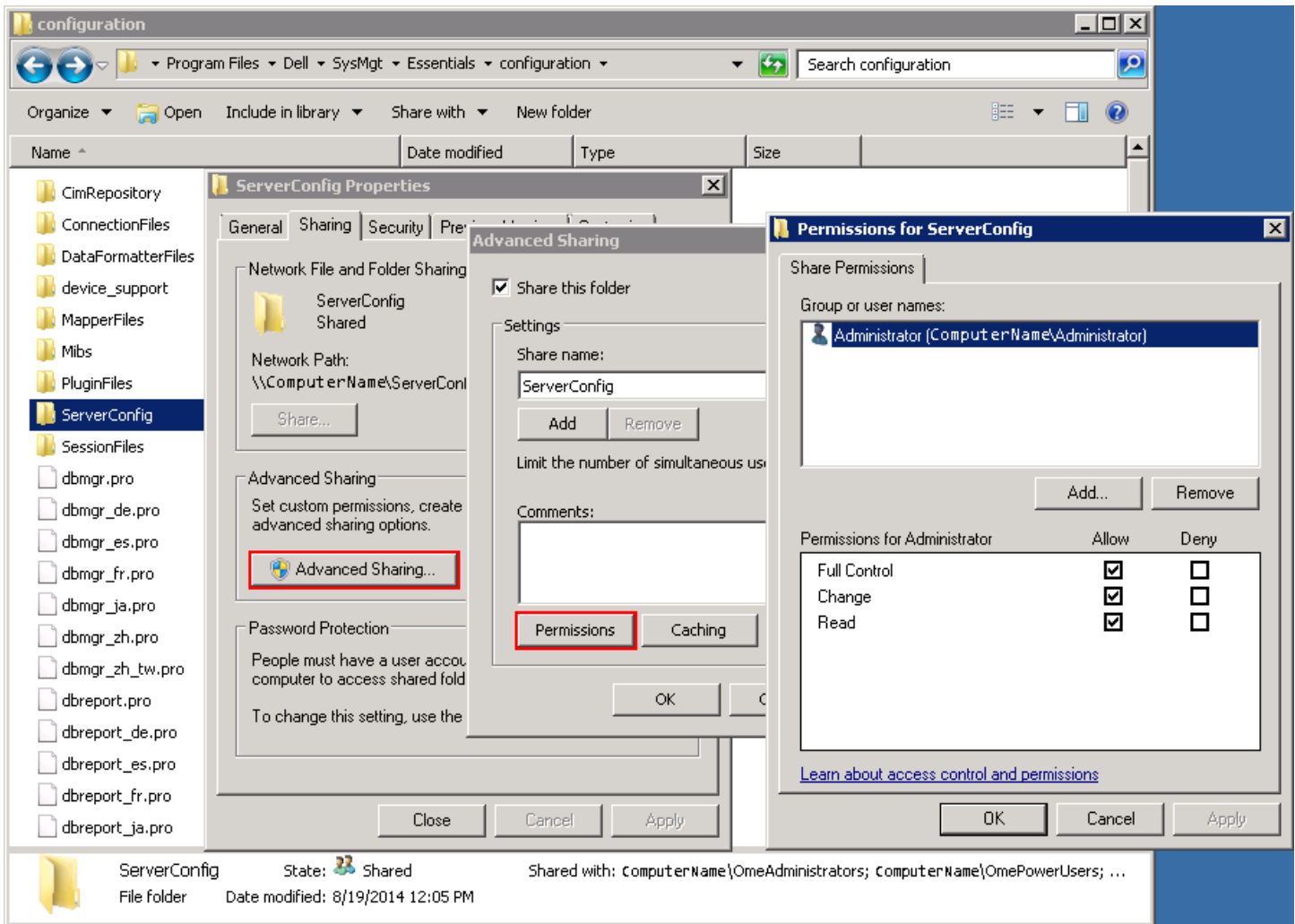
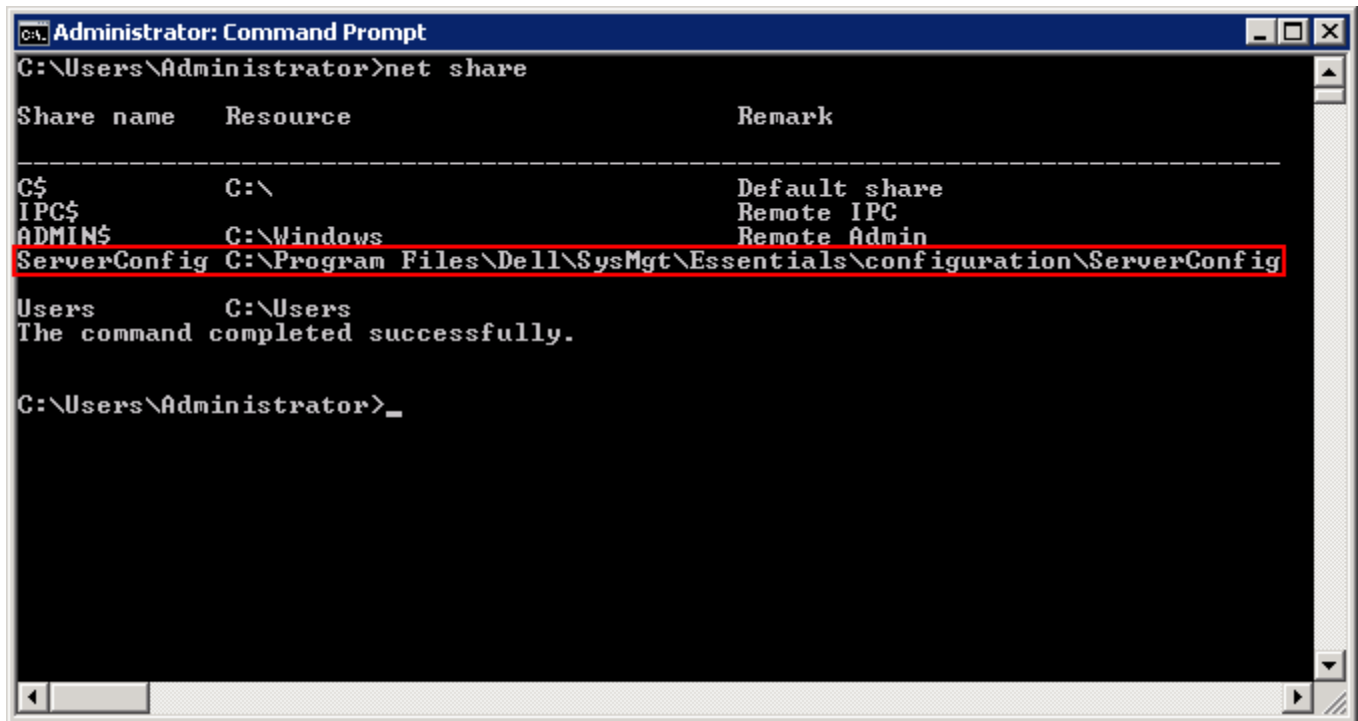


Figure 18 Advanced sharing tab of the 'ServerConfig' folder

4. Verify the share folder location using the 'net share' command.
 - a. Open the command prompt and type 'net share'.
 - b. A share with the name 'ServerConfig' should be in the network share list.



```
Administrator: Command Prompt
C:\Users\Administrator>net share

Share name      Resource                                Remark
-----
C$              C:\                                    Default share
IPC$            C:\                                   Remote IPC
ADMIN$          C:\Windows                           Remote Admin
ServerConfig    C:\Program Files\Dell\SysMgt\Essentials\configuration\ServerConfig
Users           C:\Users
The command completed successfully.

C:\Users\Administrator>
```

Figure 19 Net share command results

5. Check the user permissions in the 'User Accounts' window.

21.2 Troubleshooting creating a template

Troubleshooting creating a template from a reference device

1. Make sure that the file share settings are correctly configured. See the [How to setup the file share](#) section or the [Troubleshooting the file share](#) section.
2. Run the task again. Right click the task or task execution history and select 'Run'.
3. The task execution may have an 'LC' code in the details. Review the 'LC' code in the iDRAC documentation. See the [Additional resources](#) section below.
4. Make sure that the provided credentials have enough privileges to run the task (requires administrator privileges on the iDRAC/CMC/IOA).
5. Make sure that the minimum firmware version and supported operational mode requirements are met by the reference Dell Networking IOA device.

Troubleshooting creating a template from a file

1. Make sure the file meets the file requirements in the [File requirements](#) section.
2. If you do not see the file you are looking for, make sure the file type is correct (in the file dialogue next to file name). The available options are .xml, .ini and .txt.



21.3 Troubleshooting creating a virtual IO pool

Troubleshooting creating or editing an identity type

1. Make sure the identity type definition meets the requirements for that identity type. See the [Types of identities](#) section.
2. If you can't edit a virtual IO pool, it is likely locked. To unlock it (and enable editing) see the [How to lock or unlock a Virtual IO Pool](#) section.
3. If a virtual IO pool runs out identities to assign, a warning message appears during the assignment process in the deploy wizard. The size of a virtual IO pool can be increased. See the [How to increase the size of a Virtual IO Pool](#) section.

21.4 Troubleshooting deploying a template

The task execution history details provide troubleshooting information.

1. Check that the file share settings are entered correctly (see the [Troubleshooting the file share](#) section).
2. Double click the task execution history entry (or right click and select 'Details') to see the task execution history details. The 'Results' tab displays information on task activities and any errors that occurred. Errors with an 'LC' error code can be looked up in the iDRAC documentation (link in the [Additional resources](#) section). The details tab also contains the results of applying individual attributes.
3. If there is a 'cannot connect to server' error, make sure the target credentials are correct.
4. For a 'server is being configured' error, wait and retry later. If the task still fails, the server may need a reboot and/or iDRAC reset.
5. For a server reboot failure, reboot the server via the iDRAC interface.
6. If an attribute fails to be set, there may be an attribute dependency conflict. In some cases, re-running the task allows additional configuration settings to be applied to targets. For more details about attribute dependencies, refer to the attribute registry (link in the [Additional resources](#) section).
7. If the task does not complete, the task will timeout and exit after 30 minutes of inactivity. Rerun the task. A reboot and/or iDRAC reset may be necessary.



8. The following table lists the Dell Networking IOA operational modes and result of deployment task:

Operational mode of the IOA from which the template is created or imported	Operational mode of the IOA on which the template is deployed	Deployment Task Status
Stack	Any mode	Failed
Any mode	Stack	Failed
Standalone	Programmable MUX (PMUX)	Warning
Standalone	Standalone	Complete
PMUX	PMUX	Warning
PMUX	Standalone	Warning
Virtual Link Trunk (VLT)	VLT	Complete
VLT	Non-VLT	Failed
Non-VLT	VLT	Failed

21.5 Troubleshooting auto deploying templates

Each time the 'Deploy Configuration to Undiscovered Devices' task runs, it looks for Service Tags in the 'Auto Deployment' list. The following situations may be encountered:

1. There are no Service Tags in the 'Auto Deployment' list. In this case, the task exits, and no entry is created in the task execution history grid for that run.
2. The task finds one or more Service Tags in the 'Auto Deployment' list for devices that have not been discovered by OME yet. In this case, a task execution history entry is created and it indicates why the Service Tag was not processed.
3. The task finds one or more Service Tags in the 'Auto Deployment' list for devices that have been discovered by OME. It creates tasks named 'Deploy Configuration to Undiscovered Devices - Task – timestamp' to deploy to those devices. In this case, an execution history entry is created and the entry specifies which Service Tags were processed for deployment.
4. If an error occurs in a task created for auto deployment to a device, troubleshooting for that error should be done as explained in the [Troubleshooting the file share](#) section.



21.6 Troubleshooting deploying a network ISO

The task execution history details provide troubleshooting information.

If the network is unable to find the ISO share, check the following:

1. Verify the IP address in the share location.
2. Verify the path to the folder of the share.
 - a. A common misconception is to put the share base folder in the share name area; however, the share base folder is for the full folder path. For example:
 - i. Share: share\isos\linux File name: Ubuntu.iso (correct)
 - ii. Share: share File name: isos\linux\Ubuntu.iso (incorrect)
3. Verify the user credentials for the file share.

If the task is unable to find the file, check the following:

1. Check the file name for correctness.
2. Check the path of the ISO.

21.7 Troubleshooting configuration compliance

If a device does not show in the pie chart, make sure it meets the device configuration requirements (see the [Target device requirements](#) section).

If a device was recently licensed and shows as 'unlicensed', refresh the inventory of the device by right clicking on the device in the device view under 'Manage' -> 'Devices' and selecting 'Refresh Inventory'. After the inventory is run, the device state should no longer be 'Not Licensed'.

If a device is shown in the pie chart, follow the states in the [How to view and leverage the compliance report](#) section.

If you believe the state of a device is incorrect, refresh the configuration inventory of the device (right click the device compliance entry and select 'Run Inventory Now').



A Additional resources

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell Customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and installations.

Referenced or recommended Dell publications:

- Dell Attribute Registry:
<http://en.community.dell.com/techcenter/systems-management/w/wiki/1979.lifecycle-controller.aspx#attributereg>
- Dell iDRAC7 with Lifecycle Controller 2 White Papers:
<http://en.community.dell.com/techcenter/systems-management/w/wiki/4317.white-papers-for-idrac7-with-lifecycle-controller-2.aspx>
- Dell iDRAC Licensing:
http://en.community.dell.com/techcenter/systems-management/w/wiki/3204.dell-remote-access-controller-drac-idrac.aspx#iDRAC7_licensing
- Dell LC Error Codes:
<http://en.community.dell.com/techcenter/systems-management/w/wiki/1979.lifecycle-controller.aspx>
- Dell OpenManage Essentials TechCenter page:
<http://en.community.dell.com/techcenter/systems-management/w/wiki/1989.openmanage-essentials.aspx>



B Boot-from-SAN Considerations

The attributes for a template include attributes to support Boot-from-SAN operations. Boot-from-SAN functionality may run over iSCSI, FC, or FCoE connections. Attributes for Boot-from-SAN operations include attributes for both initiators and targets.

Regardless of the protocol being used, the storage (target) hardware and software must be setup, configured, and available on the network. It is beyond the scope of this document to address this topic, as these procedures are usually vendor-specific.

In order for a device to be able to boot-from-SAN, its attributes must be correctly configured. When using manual identity assignment, the operator is responsible for setting all attributes to appropriate values. When using OME's auto identity assignment, OME uses the Virtual IO Pool associated with a Compute Pool to set applicable Initiator identity attributes associated with Boot-from-SAN operations. If Target attributes for Boot-from-SAN operations need to be changed (e.g., to use a different target), the operator has to make those changes manually.

Boot-from-SAN Using iSCSI

The following attributes apply to Boot-from-SAN operations using iSCSI:

Initiator Attributes

General iSCSI Attributes

- iScsiOffloadMode
- TcpipViaDHCP
- IscsiViaDHCP
- DhcpVendId
- ChapAuthEnable
- ChapMutualAuth
- LnkUpDelayTime
- LunBusyRetryCnt
- IpVer
- IpAutoConfig
- TcpTimestmp
- WinHbaBootMode

Initiator-Specific iSCSI Attributes

VirtIscsiMacAddr

- IscsiInitiatorIpAddr, IscsiInitiatorIpv4Addr, IscsiInitiatorIpv6Addr
- IscsiInitiatorSubnet
- IscsiInitiatorSubnetPrefix
- IscsiInitiatorGateway, IscsiInitiatorIpv4Gateway, IscsiInitiatorIpv6Gateway
- IscsiInitiatorPrimDns, IscsiInitiatorIpv4PrimDns, IscsiInitiatorIpv6PrimDns



IscsiInitiatorSecDns, IscsiInitiatorIpv4SecDns, IscsiInitiatorIpv6SecDns
IscsiInitiatorName
 IscsiInitiatorChapId
 IscsiInitiatorChapPwd
 IscsiVlanMode
 IscsiVlanId
 SecondaryDeviceMacAddr
 UseIndTgtPortal
 UseIndTgtName
 Related Attributes
 BiosBootSeq
 BootOption
 VirtualizationMode

Target Attributes

General Target iSCSI Attributes

IscsiTgtBoot
 ConnectFirstTgt ConnectSecondTgt
 FirstHddTarget

Target-Specific iSCSI Attributes

FirstTgtIpVer	SecondTgtIpVer
FirstTgtIpAddress	SecondTgtIpAddress
FirstTgtTcpPort	SecondTgtTcpPort
FirstTgtIscsiName	SecondTgtIscsiName
FirstTgtBootLun	SecondTgtBootLun
FirstTgtChapId	SecondTgtChapId
FirstTgtChapPwd	SecondTgtChapPwd

Of the preceding iSCSI attributes related to boot-from-SAN, the only ones assigned by OME, for automatic identity assignment, are the **VirtIscsiMacAddr** and **IscsiInitiatorName** attributes (highlighted above). A value for the **VirtIscsiMacAddr** attribute is obtained using the “Ethernet Identities” definition specified for the Virtual IO Pool, and a value for the **IscsiInitiatorName** attribute is obtained using the “iSCSI IQN Identities” definition given for the Virtual IO Pool.

OME 2.1 has the following limitation regarding iSCSI boot-from-SAN and auto-assignment of identity values from a Virtual IO Pool:

- Support is only provided for the assignment of iSCSI IP addresses by DHCP, which is specified via the following two attributes and corresponding values:

TcpipViaDHCP	“Enabled”
IscsiViaDHCP	“Enabled”



Due to this restriction, Virtual IO Pools don't have a provision for assigning IP addresses, subnet, or gateway values for iSCSI.

Boot-from-SAN Using FC/FCoE

The following attributes apply to Boot-from-SAN operations using FC/FCoE:

Initiator Attributes

VirtWWN
VirtWWPN
VirtFIPMacAddr

Target Attributes

General Attributes

FCoEOffloadMode
FCoETgtBoot
ConnectFirstFCoETarget
FCoELnkUpDelayTime
FCoELunBusyRetryCnt
FCoEFabricDiscoveryRetryCnt
FCoEBootScanSelection
BootOrderFirstFCoETarget
BootOrderSecondFCoETarget
BootOrderThirdFCoETarget
BootOrderFourthFCoETarget

Target-Specific Attributes

FirstFCoEWWPNTarget
FirstFCoEBootTargetLUN
FirstFCoEFCFVLANID
FCoEFirstHddTarget

Of the preceding FC/FCoE attributes related to boot-from-SAN, the only ones assigned by OME, for automatic identity assignment, are the **VirtWWN**, **VirtWWPN**, and **VirtFIPMacAddr** attributes (highlighted above). A value for the **VirtWWN** attribute is obtained using the "FCoE Node Name Identities" definition specified for the Virtual IO Pool, a value for the **VirtWWPN** attribute is obtained using the "FCoE Port Name Identities" definition specified for the Virtual IO Pool, and a value for the **VirtFIPMacAddr** attribute is obtained using the "Ethernet Identities" definition given for the Virtual IO Pool.

