DELL Technologies

Technical White Paper

Profile Management and Deployment Enhancements in OpenManage Enterprise 3.4

Abstract

OpenManage Enterprise (OME) 3.4 has a new Profile Management portal which enables users to easily replace systems in a data center and to apply changes efficiently. OME 3.4 also significantly enhances the configuration and deployment capabilities and has intelligent identity assignment logic. Read on to know more.

September 2020

Revisions

Date	Description
September 2020	Initial release

Acknowledgements

Authors: OpenManage Enterprise (OME) Engineering

[Pushkala Iyer, Reg Stumpe, Rakesh Ayola, Gabe Stern]

Table of contents

Executive summary

OpenManage Enterprise 3.4 has significant improvements in the Configuration and Deployment domain. There is a new Profile Management portal enabling users to view, modify, and deploy profiles. This enables users to generate profiles upfront and enables easy migration and part-replacement. Virtual identity allocation logic is intelligent - the assignment avoids identities that have been externally allocated. OME 3.4 enables deployment of secure and quasi target specific attributes to systems. There are also significant improvements in managing deployments to OME-M sleds specifically with respect to network definitions. Read on to know more about these exciting new features in OME 3.4.

1 Background and Overview

This technical white paper outlines how OME 3.4 addresses many feature gaps and customer issues in device Configuration and Deployment. The following are the key features that are implemented and the customer issues that have been addressed:

- Profile Management Portal
  - Ability to generate profiles with settings and virtual identities for deployment to a device that are discovered or yet to be discovered using Service Tag.
  - Ability to easily view what was deployed to a device (settings and virtual identities).
  - Ability to easily view what has changed on the profile since the last deployment.
  - Ability to deploy just the delta or change-set on the profile only. Thereby, reducing overall deployment time.
  - Problem-free part replacement using full redeployment of profile.
  - Easier server retirement or replacement via unassign and assign of a profile or migrate profile actions.
- Boot Attribute deployment without caveats
  - Previous releases had the restriction that to deploy boot attributes, a template had to be associated with an identity pool and boot attributes could only be seen in the context of identity reservation. In previous releases, boot attributes could not be included for configuration compliance either.
- Deployment covers all attributes
  - In previous releases, deployment did not include secure or target specific attributes. The only target specific attributes that were supported were the virtual identity attributes.
- Intelligent Identity pools
  - Identity pool definitions are not fixed, so it is possible that there are intersections with pool definitions in other OME instances or other consoles. Previously, OME was unable to detect any externally assigned identity intersection with identity pools and so could potentially inadvertently cause a virtual identity conflict.
- Easier workflows to manage OME-M sleds
  - In previous releases, when OME was used to manage multiple MX-7000chassis, the workflows involved repetitive steps to re-create networks on OME. OME-M Sleds would also need to be rebooted to apply VLAN changes as applying VLAN changes was tightly integrated with template deployment.

1.1 Audience

The information in this white paper is intended for users who have some familiarity with the OME Configuration and Deployment workflows for template creation, identity pool creation, template deployment, configuration compliance, and so on. For comprehensive detail of all these features, see the OpenManage Enterprise 3.4 User's guide and OpenManage Enterprise Version 3.4 and OpenManage Enterprise – Modular Edition Version 1.20.00 RESTful API guide.

2 Configuration and Deployment improvements in OME 3.4

2.1 Profile Management using the Profile Portal

OME 3.4 has a new Profile Management Portal as seen in the screenshot below.

A Profile provides a mechanism for reserving identities and establishing deployment images in advance, for use in deployment later.

When a profile is created, applicable virtual identity attribute values are reserved for it. Those assigned identity values are owned by the profile and remain with that profile for as long as it exists.

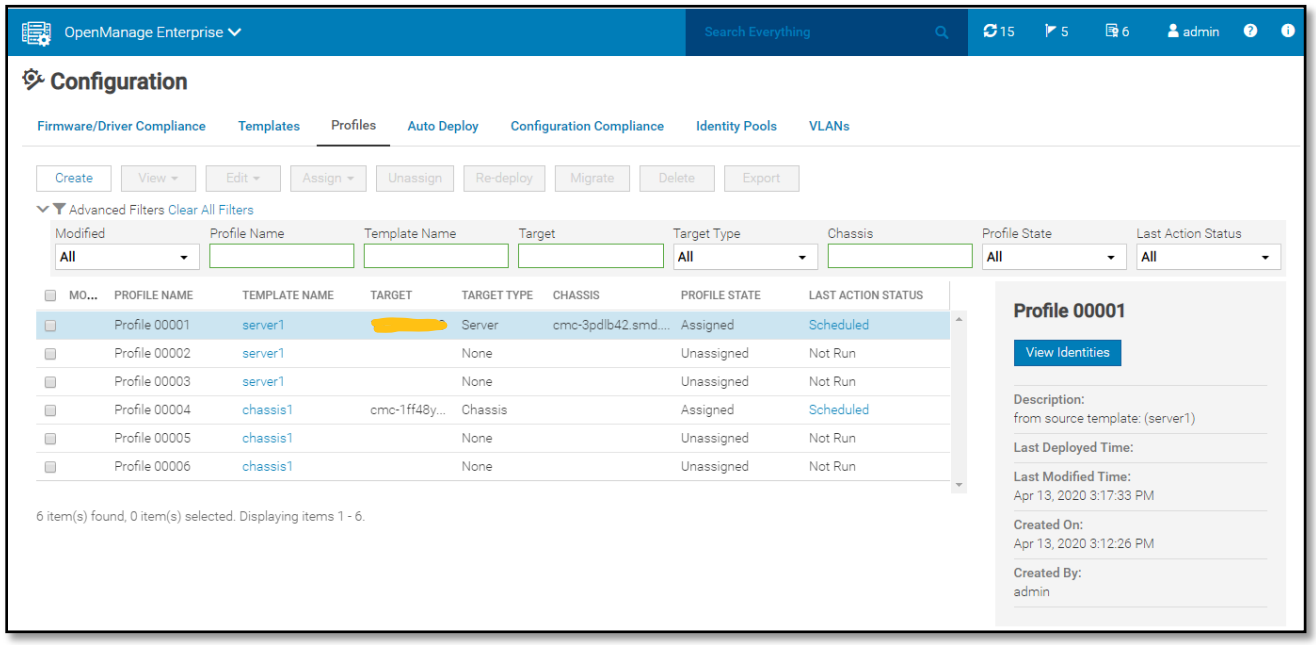

Figure 1 The Profile Management portal showing a list of profiles

The profile portal provides a multitude of functionalities, as seen from the menu options.

- Creation of reserved or unassigned profiles with virtual identities for future deployment (Create Profile).
- An easy way to view what is configured on a device (Edit Profile).
- Virtual identity management using the profiles – as virtual identities reside with the profiles (Assign or Unassign)
  - Decommissioning systems and replacing them with new ones is so much easier.
  - Addresses previous release limitations with migration where the settings can be unassigned from a source system and maintained with the profile before assignment to an appropriate target server.
- Ability to deploy only what is changed via **Redeploy**
  - Reduces deployment time and keeps results limited to what was explicitly changed.

- Ability to deploy the entire profile with **Deploy** or **Redeploy**
  - Useful for part-replacement scenarios. To ensure that all the settings are correctly reapplied on the system.
- Auto-Deploy has been integrated with the Profiles Portal page – a profile can be auto-deployed to a service tag.

The following state diagram shows the various profile states and transitions.

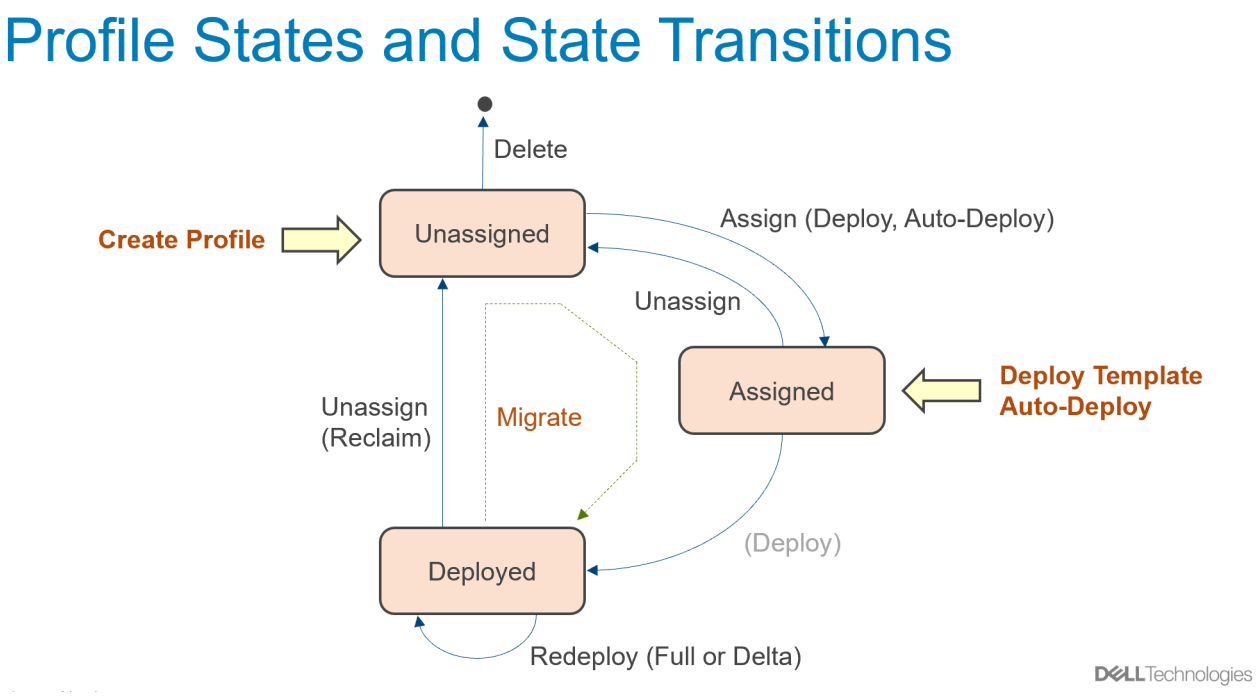

Figure 2 Profile States and Transitions

The following screenshots illustrate each of these workflows. For brevity, only the most relevant screens in a workflow are included. For more information about the feature, see OME 3.4 User's Guide.

2.1.1 Create Profiles

Create reserved profiles (unassigned) profiles by choosing a template and indicating how many profiles are needed. If the template has identity attributes, it must be associated with an identity pool.

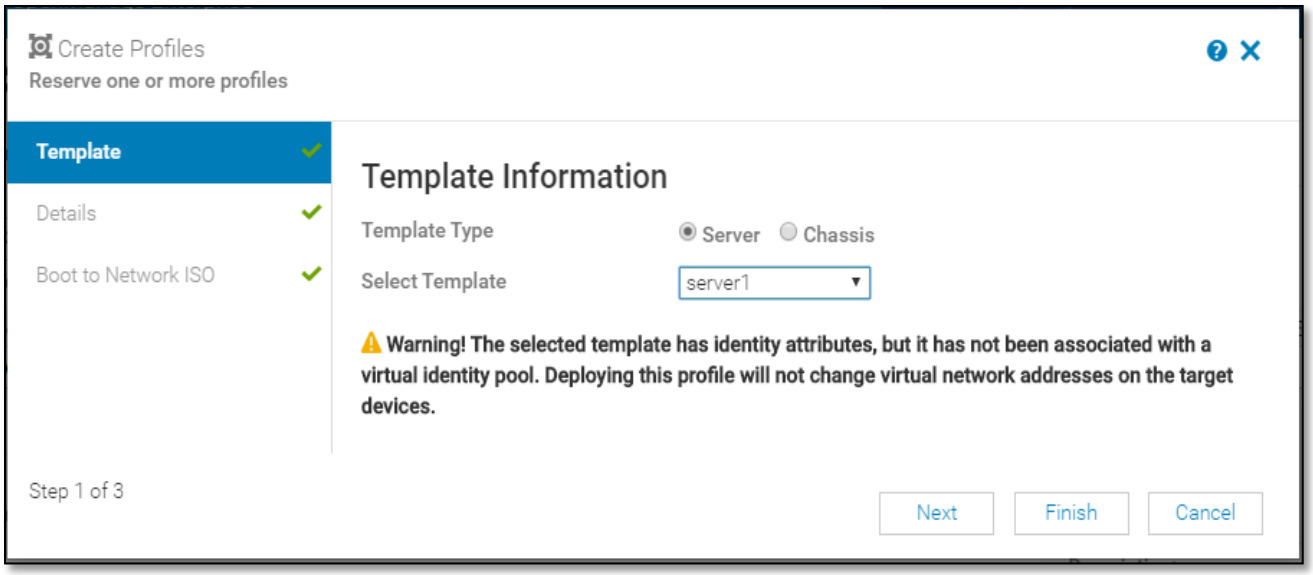

Figure 3 Profile Creation Steps: Select template information

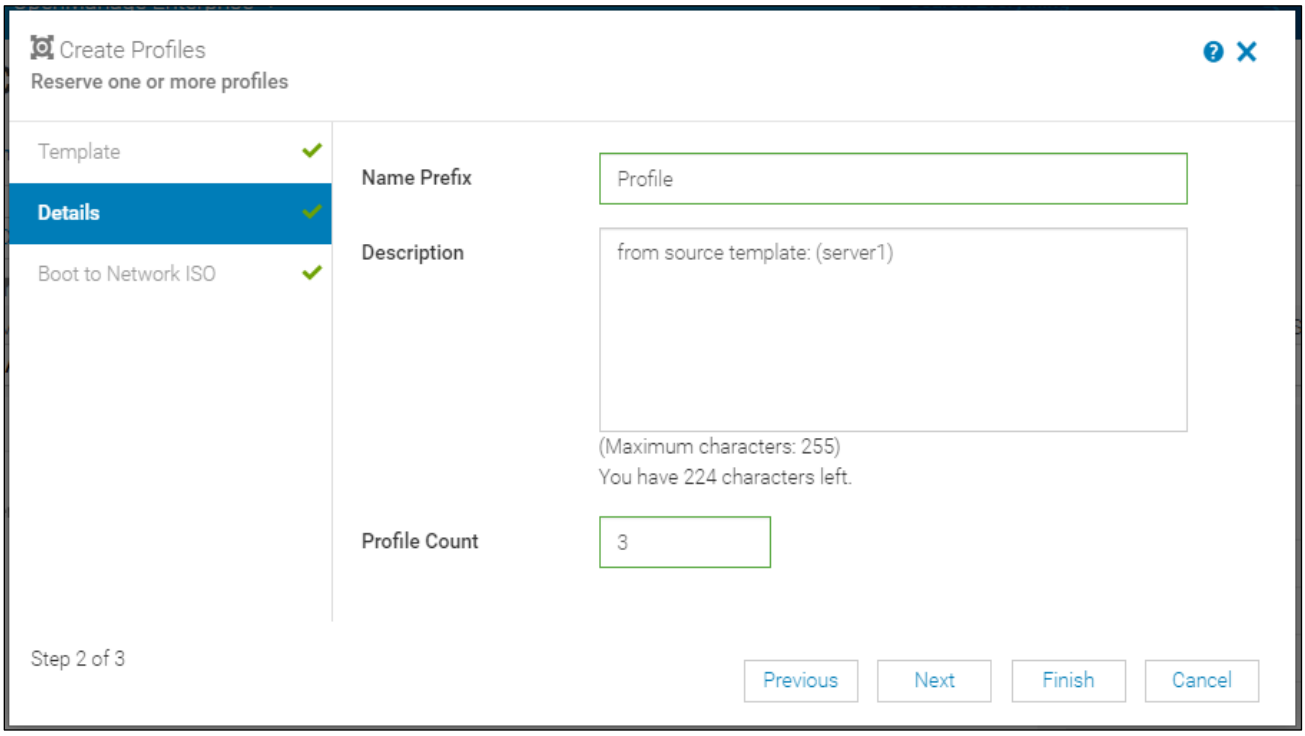

Figure 4 Profile Creation Steps: Specify name prefix and number of profiles to be generated

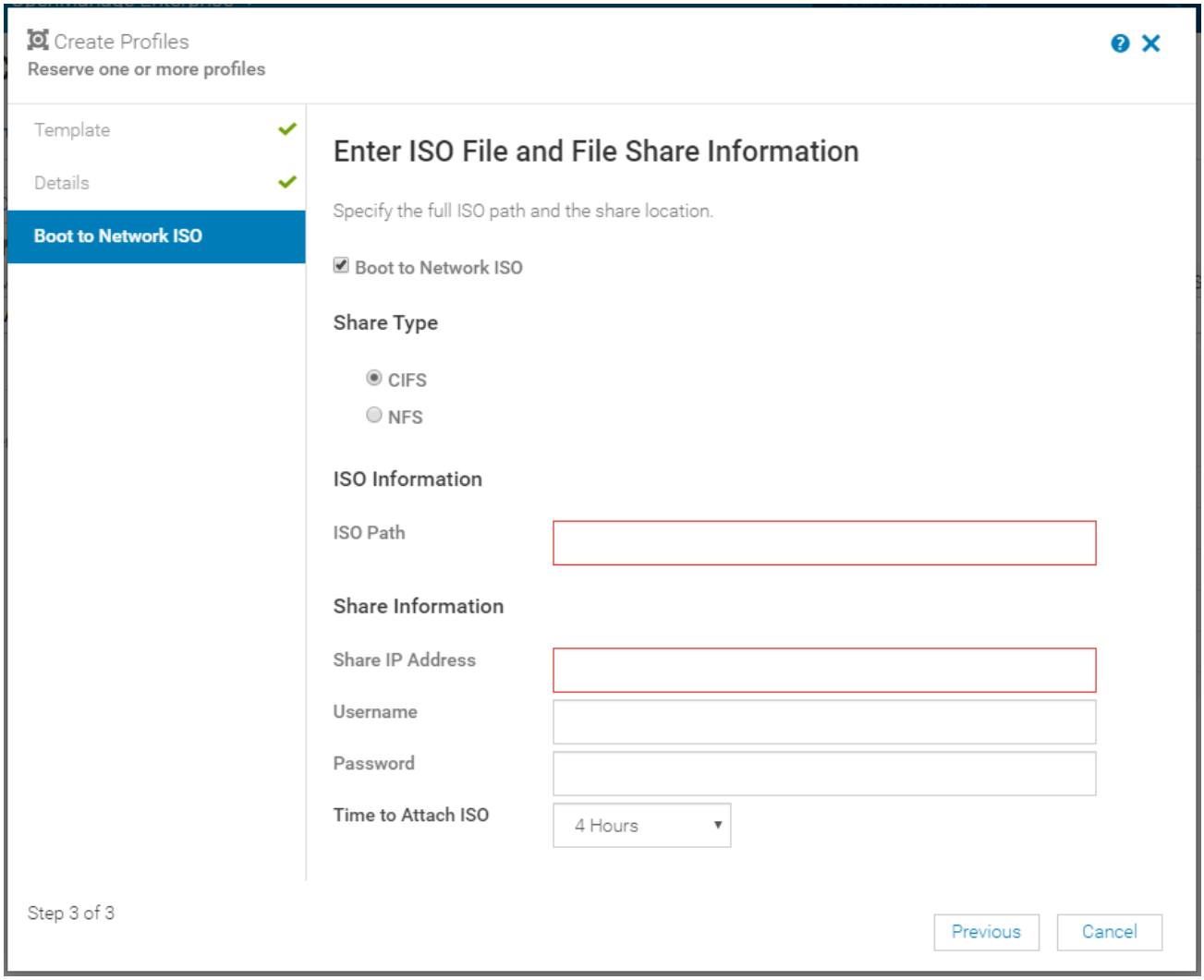

Figure 5 Profile Creation Steps: If booting to a network ISO after deployment is desired, specify full ISO path and share location

2.1.2 Deploy Profiles

Once a profile is created, it can be assigned to a device via deployment or to a service-tag via auto-deployment.

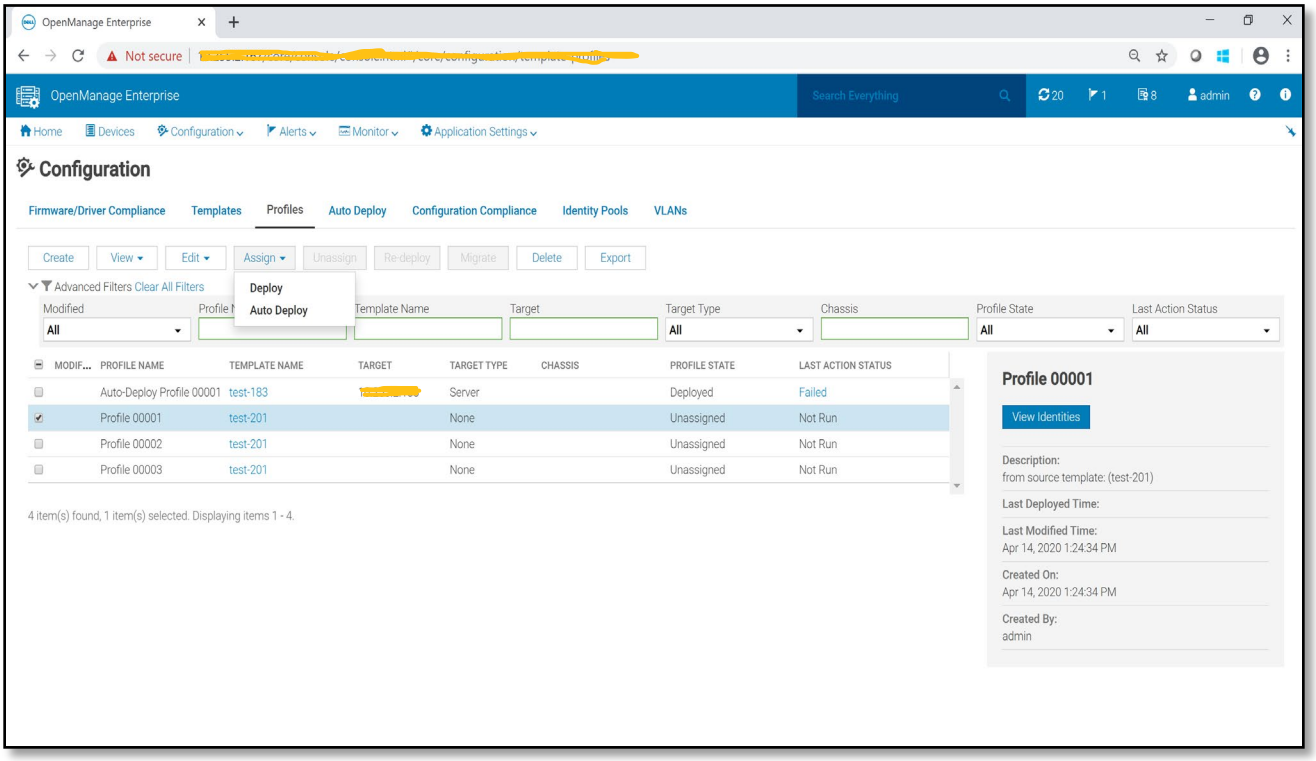

Figure 6 Profile assignment: A profile can be assigned to a device (via Deploy) or a service-tag (via Auto-Deploy)

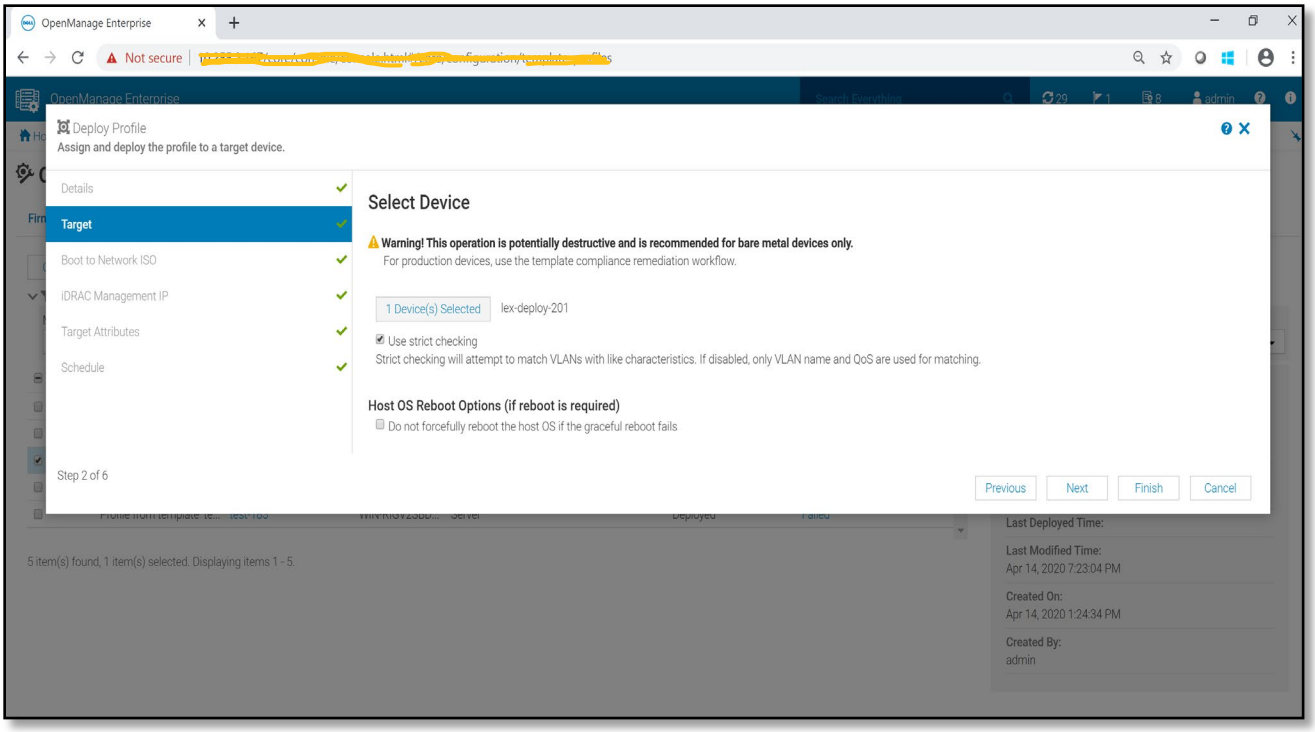

Figure 7 Profile Assignment via Deploy: A target device should be selected to deploy the profile

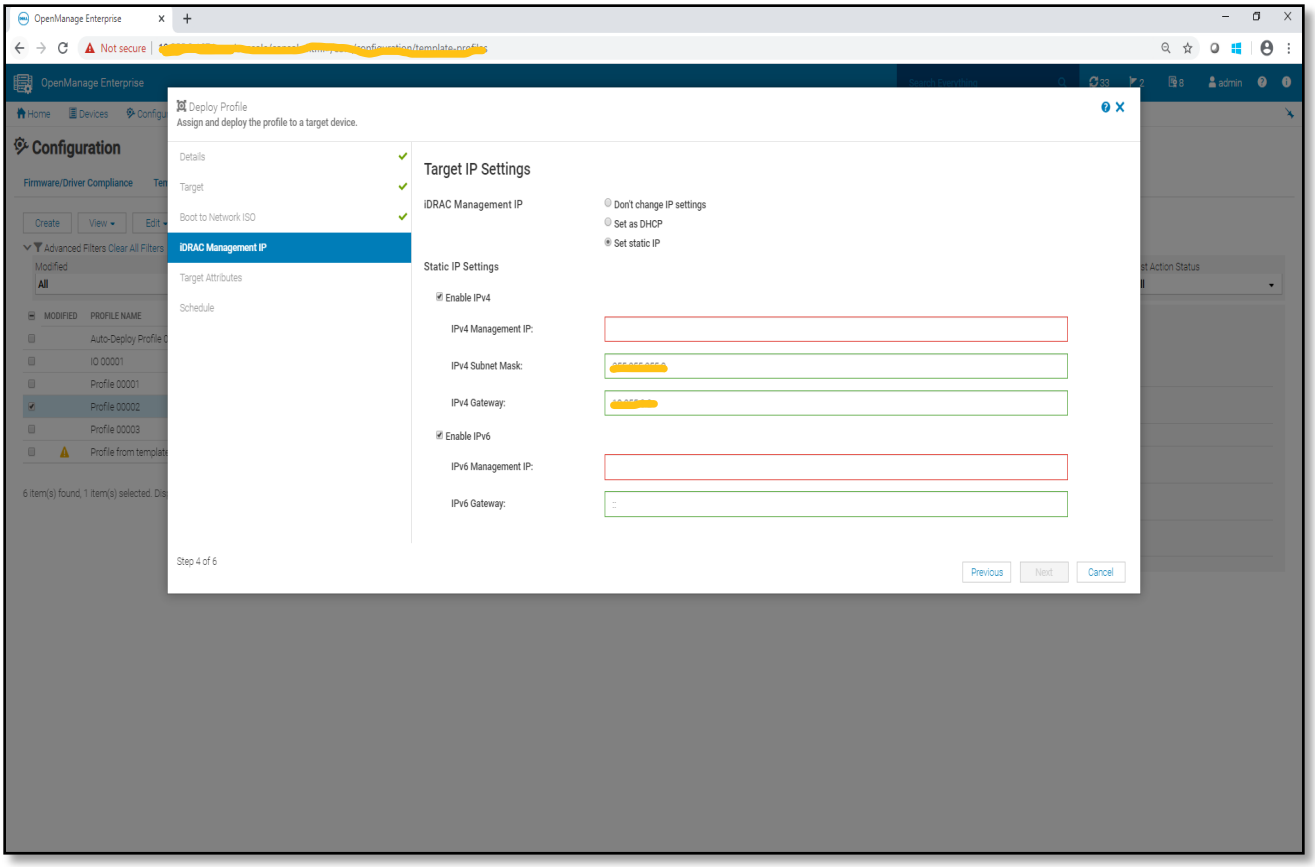

Figure 8 Profile Assignment via Deploy: Specifying IP settings for target – both IPv4 and IPv6 settings can be supplied.

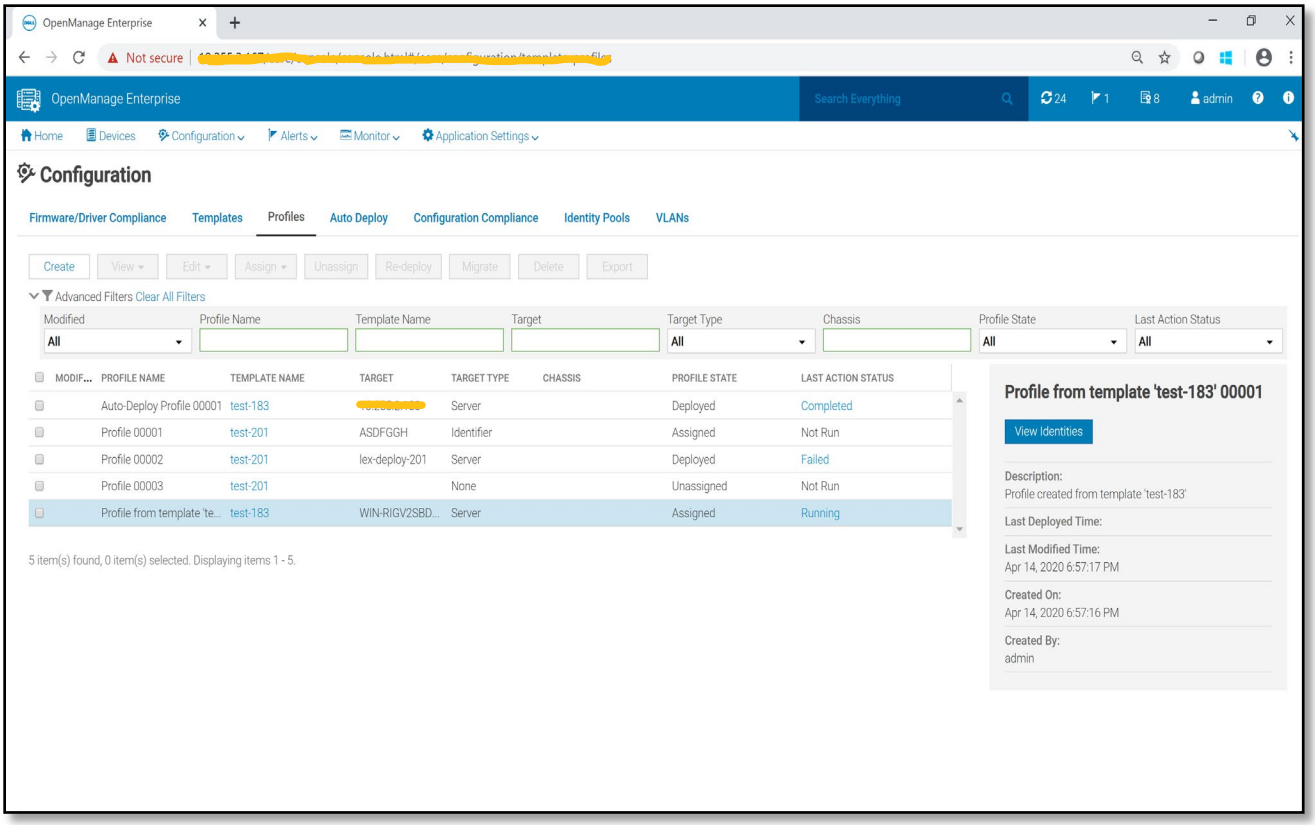

Figure 9 Profile portal showing that the profile is now “Assigned” and the deployment job is currently running

2.1.3 Edit Profiles

Edit a profile to change any of the target specific attribute values (except virtual identity attribute values).

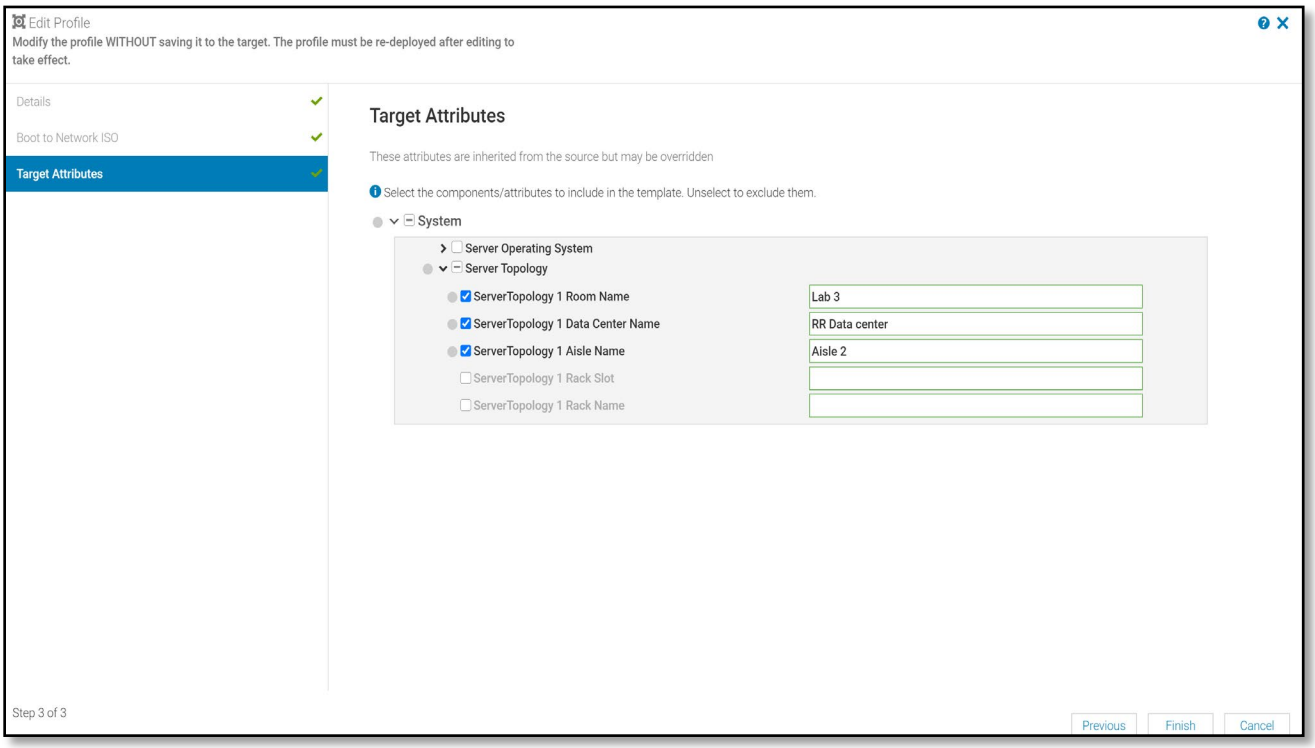

Figure 10 Edit profile: Allows change of any target specific attribute values except virtual identities

If the profile has been edited after deployment, then the profile grid displays an indicator (yellow bang) showing that it has been modified. This indicator is also displayed if the template from which the profile was created is modified.

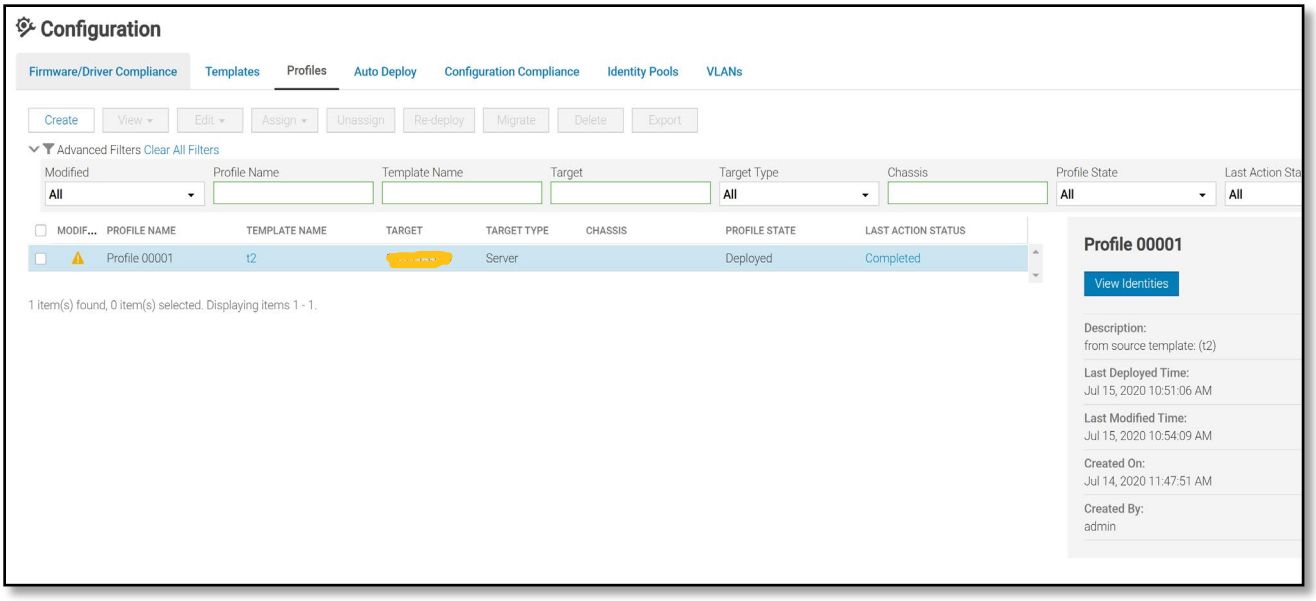

Figure 11 Profile grid showing a modified profile. The indicator is shown if either the profile (target attributes) or the source template (from which the profile was created) attributes were modified.

2.1.4 Re-deploy Profiles

A modified profile can be redeployed to the system. Users can specify if they want to deploy only the change-set (Modified attributes only—This option is useful for quick deployment) or the entire profile (the “All Attributes” option is useful for part replacement scenarios).

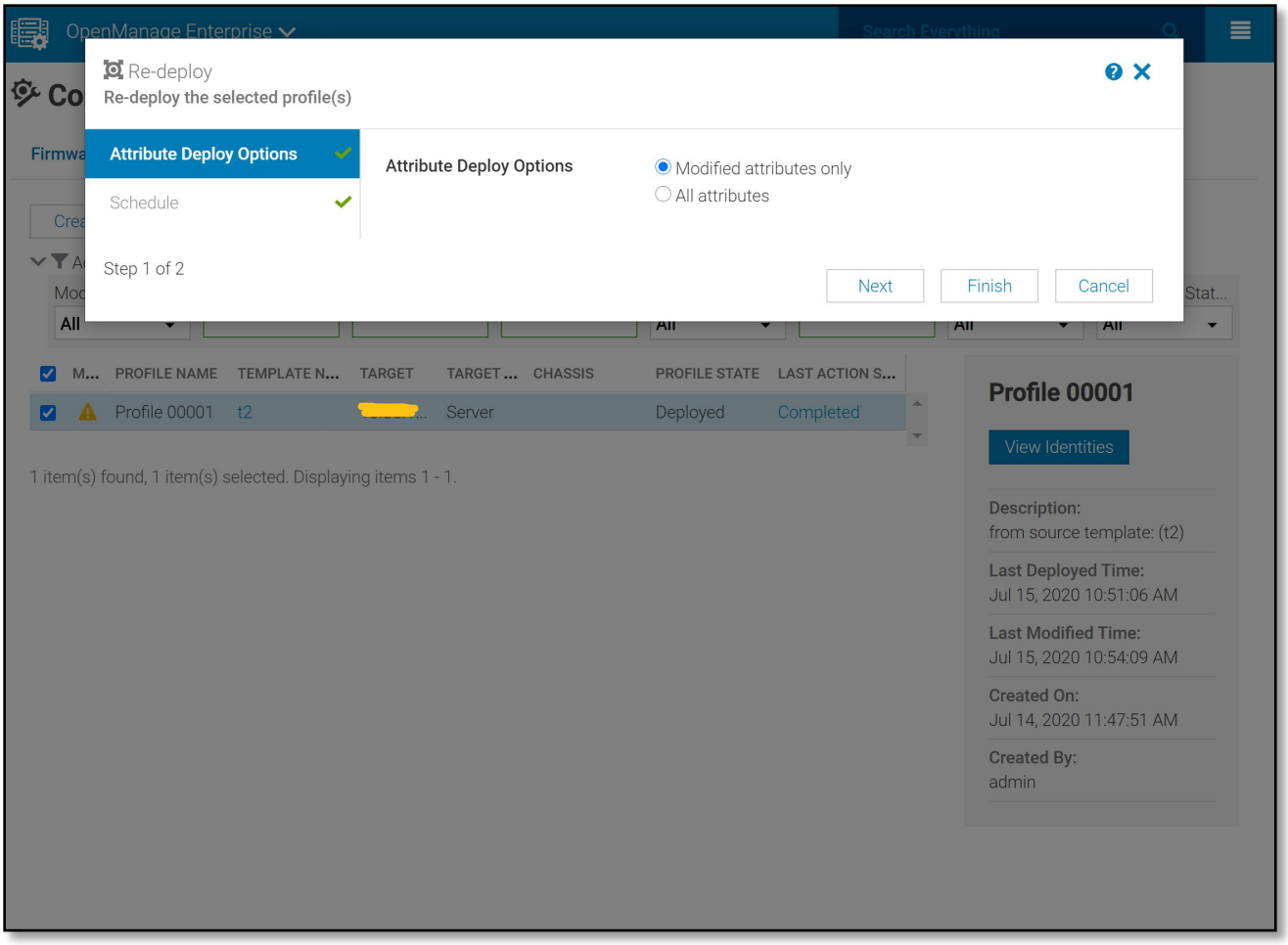

Figure 12 Options for re-deployment of a modified profile

2.1.5 Migrate Profiles

When it is time to retire a server, the migrate wizard can be used to move the profile, including all settings and virtual identities, to its replacement. The 'Force' option can be used to move the profile even when the source system is no longer available.

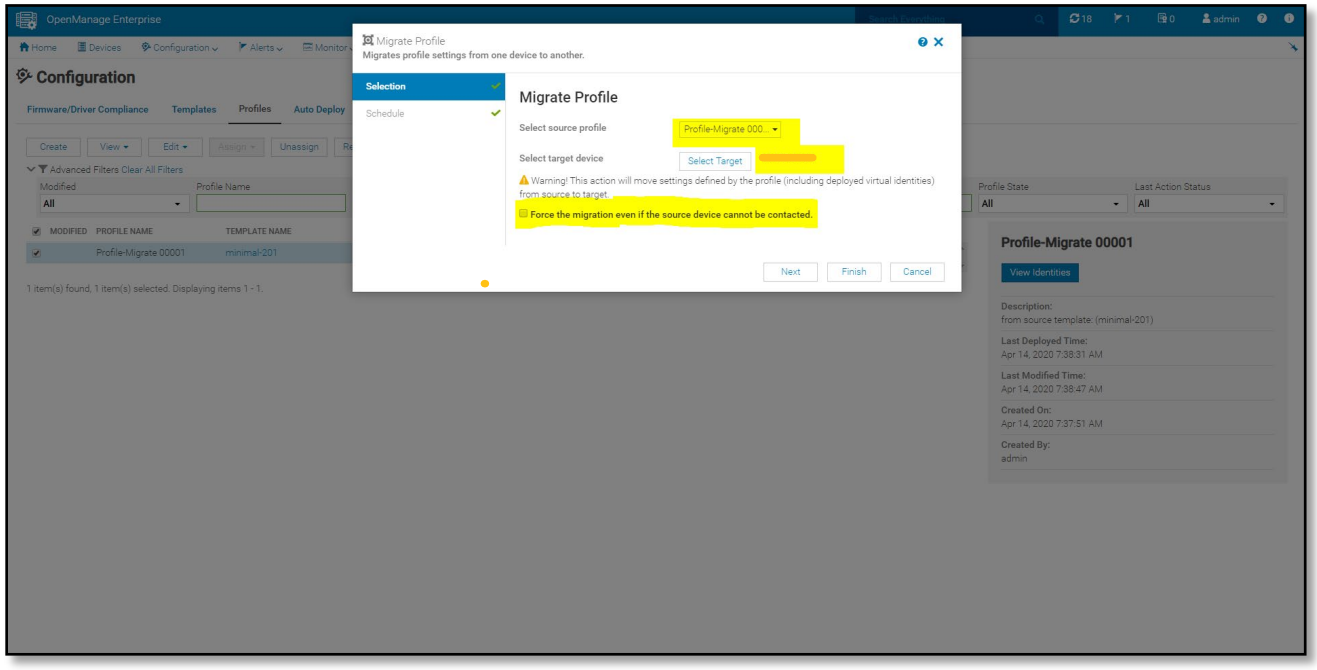

Figure 13 Options to migrate a profile.

2.2 Comprehensive Deployment Covering Target and Secure Attributes

Attributes involved in server configuration can be broadly classified into template attributes and target attributes.

The value of a template attribute is always tied to the template and gets deployed to every target device whenever a profile created from the template is used for deployment. Changes to template attributes affect every profile created from the template.

The value of a target attribute is tied to a target device, so it is specific to each target device that a profile is deployed to. Target attributes can be further classified into:

- Virtual identity attributes: Values assigned automatically by OME identity assignment logic.
- Quasi attributes: Values are inherited from the source template but can be modified on a per-target basis.
- True target attributes: Values should be uniquely specified per deployment target.

In previous OME releases, there was no support for quasi or true target attributes in deployment. Only template and virtual identity attributes could be deployed. Quasi attributes could also not be used to check compliance. Several boot control attributes are Quasi attributes. In OME 3.4, quasi attributes inherit values from the source system (from which the template is captured) and can be deployed. Also, the compliance can be evaluated for these attributes.

In previous OME releases, secure attributes (these are typically password attributes) were not deployed. In OME 3.4, these attributes are processed differently and deployed separately using different API calls. Secure attributes are not included for compliance.

The following screens show edit, save, and deployment of secure attributes:

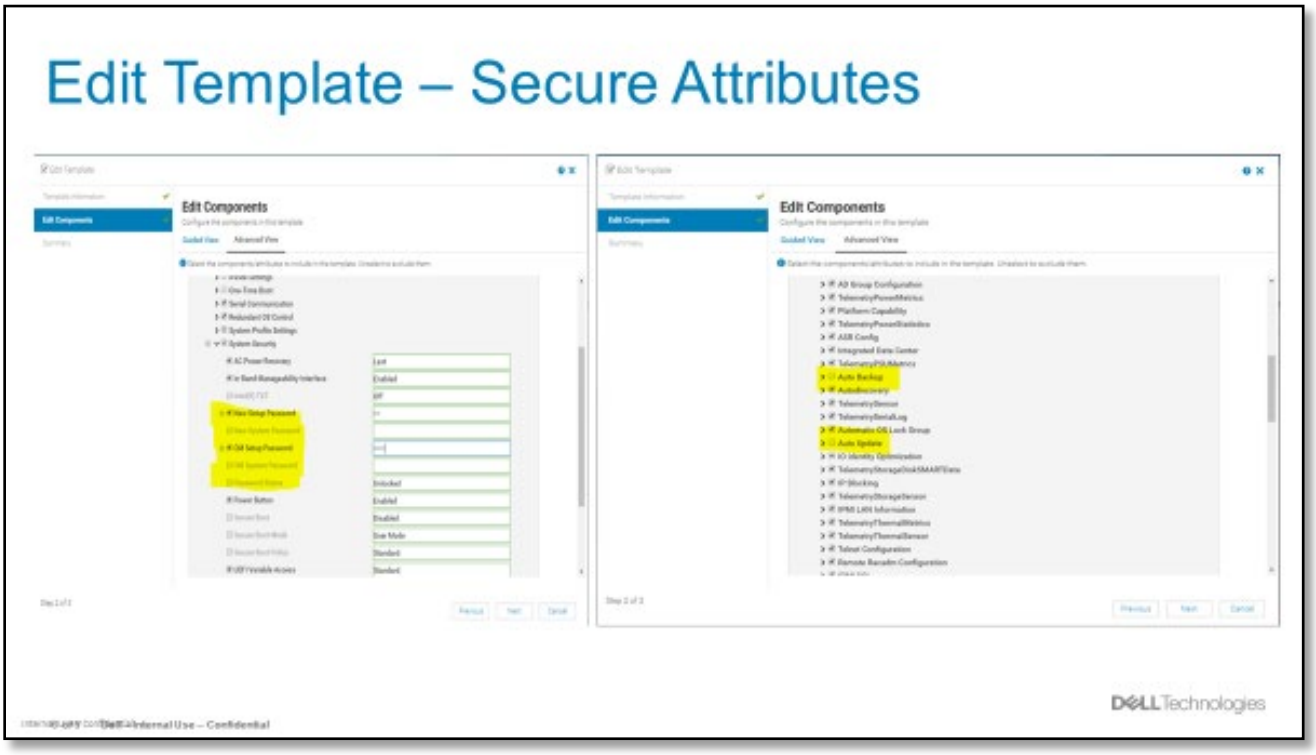

Figure 14 Ability to edit a template and supply values for secure attributes

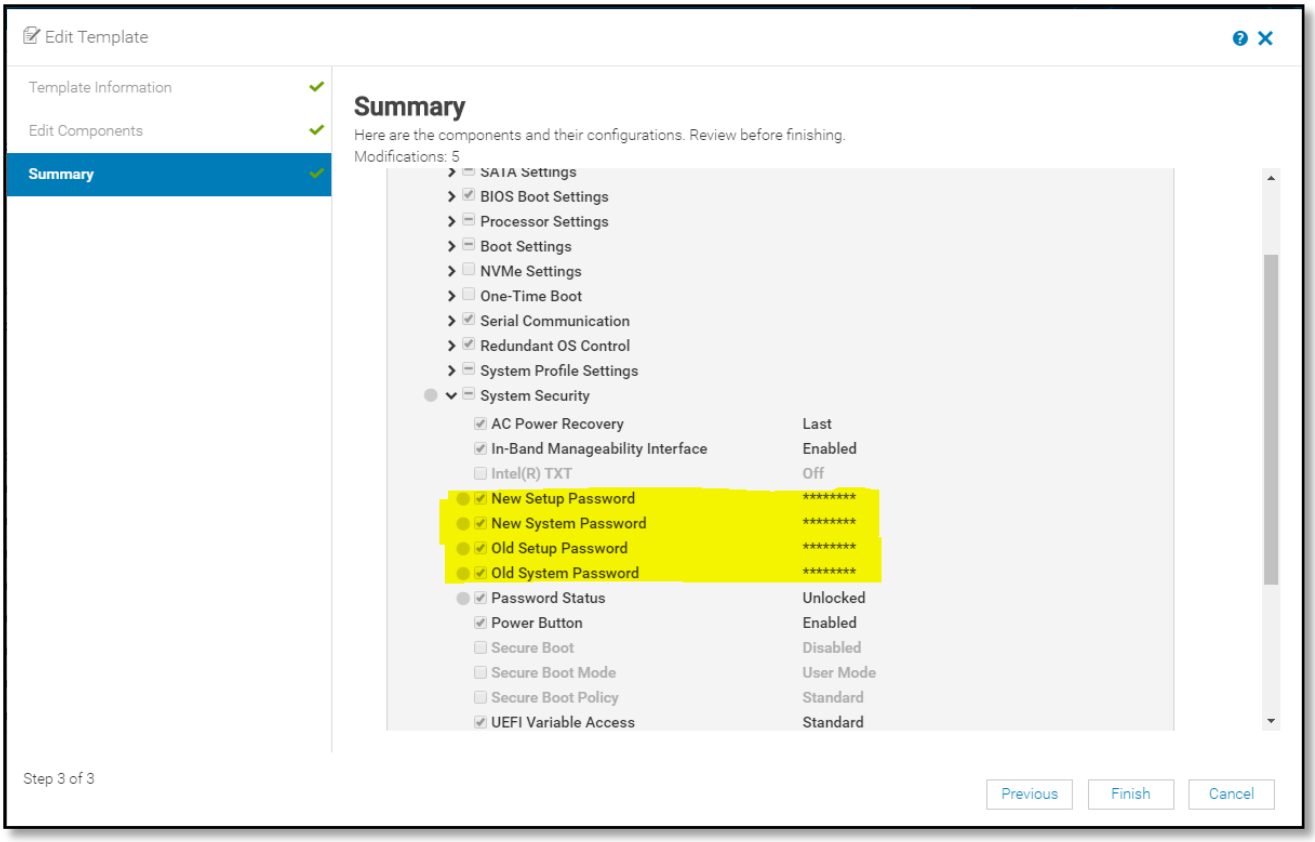

Figure 15 After values have been supplied for secure attributes

2.3 Intelligent Identity Pools

With versions prior to OME 3.4, the virtual identity assignment is unaware of possible conflicts. A conflict can exist if another console has assigned virtual identity values that intersect with identities in pools defined in OME.

In OME 3.4, if the console detects that a device already has virtual identities that intersect with pool definitions in the console, then those virtual identities are marked as already “assigned” and not used in identity assignment logic. If the virtual identities were already assigned out by the console before the externally assigned identities were detected, the device with the duplicate identities is indicated as “In conflict”. Devices with “In conflict” virtual identities can be brought out of conflict by deploying a new template to them.

The screenshots below show “In Conflict” virtual identities as seen in the identity pool usage screens.

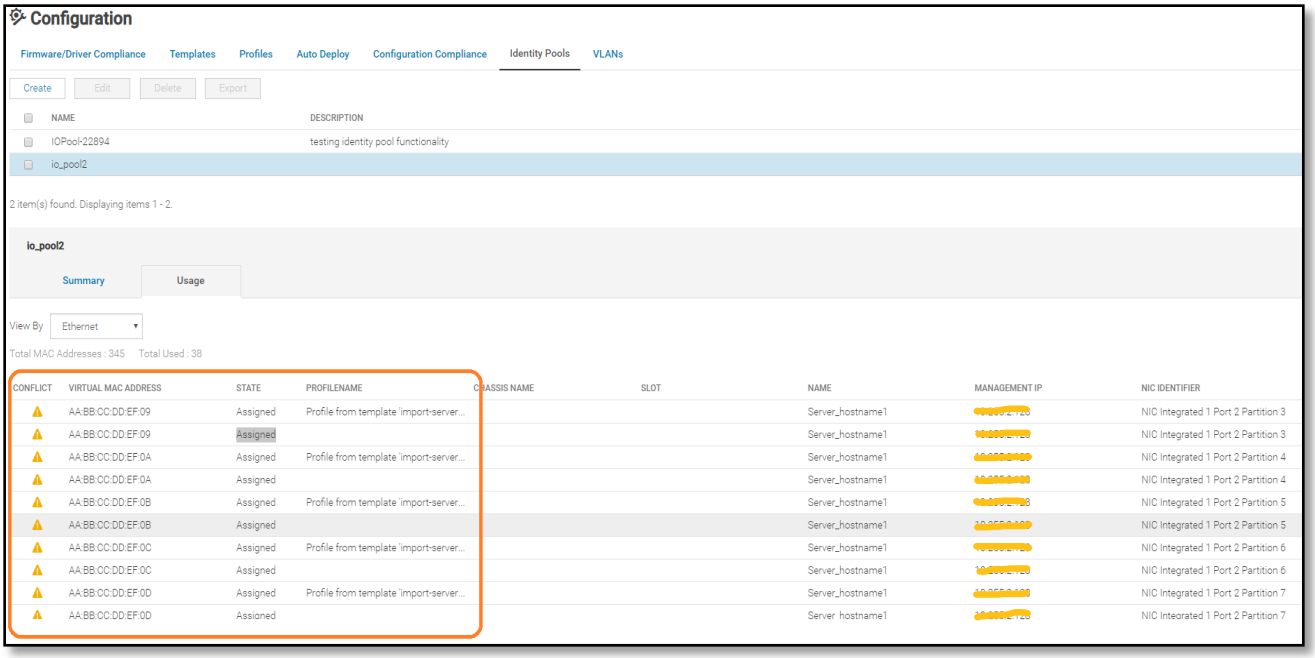

Figure 16 Identity pool usage: Virtual identities that are in conflict are displayed with a “conflict” icon

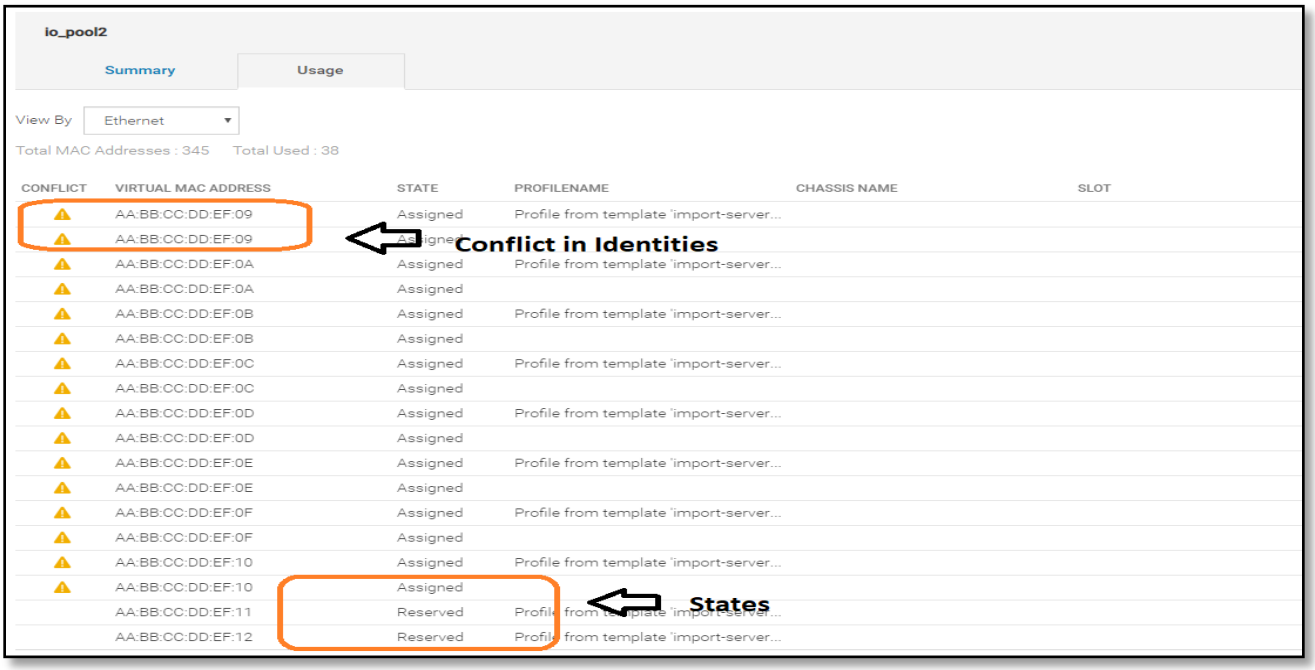

Figure 17 Identity pool usage: Virtual identities that are in conflict are displayed with a “conflict” icon, the conflict can apply to virtual identities that were previously reserved also.

2.4 Easier Workflows to Manage OME-M Sleds

Using OME 3.3 and prior versions to manage several MX7000s involved arduous network management.

Fabric management and uplink configuration are functions of the chassis element manager, users go through the following sequence of operations in OME-M.

1. Create networks by specifying name, description, VLAN ID, or range / QoS.
2. Create fabric design definitions by choosing a pair of applicable IOMs.
3. Configure uplinks for the fabric by specifying uplink type, switch ports, and the networks to use for untagged or tagged networks.

If the user preferred to use OME for template deployment and network configuration of MX7000 sleds, then the user would need to replicate network configuration (as in Step 1) in OME. In OME 3.3 and prior releases, the user would need to create the network definitions one at a time, this is time consuming and not convenient when dealing with more than 10 networks.

In OME 3.4, users can import networks into OME simply by targeting an MX7000 chassis or by importing the networks from a file.

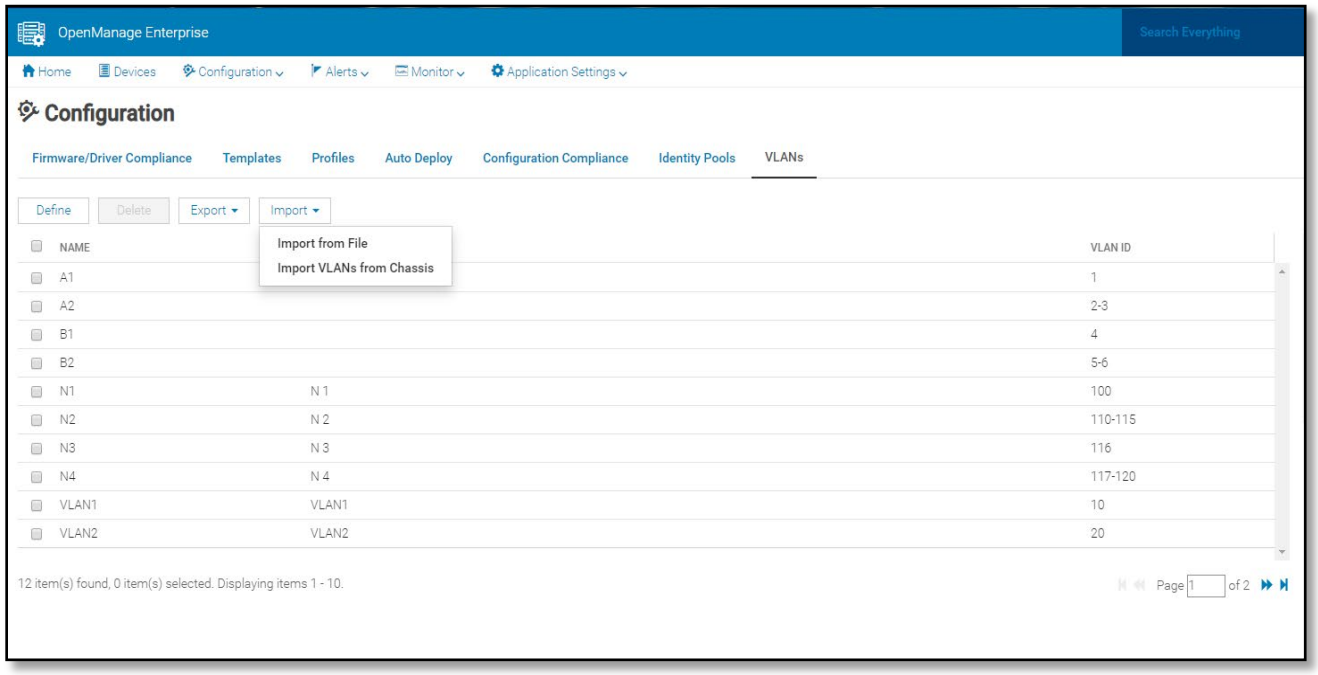

Figure 18 Easier OME-M workflows: The Import network definitions feature

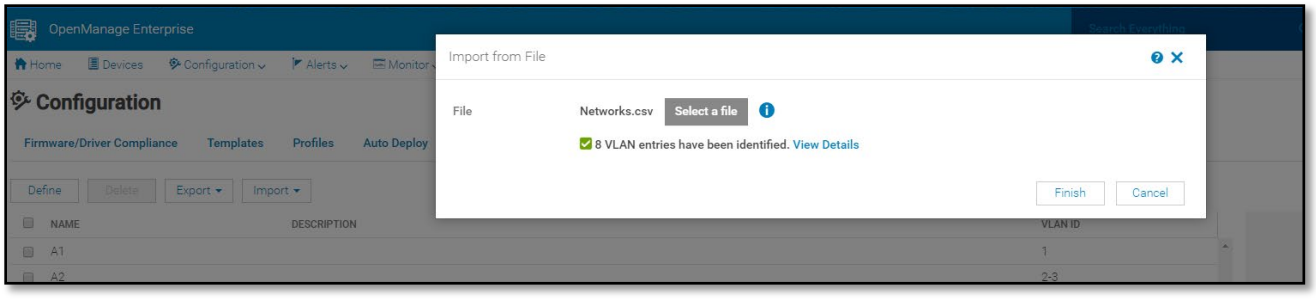

Figure 19 Easier OME-M workflows: Importing network definitions from a file

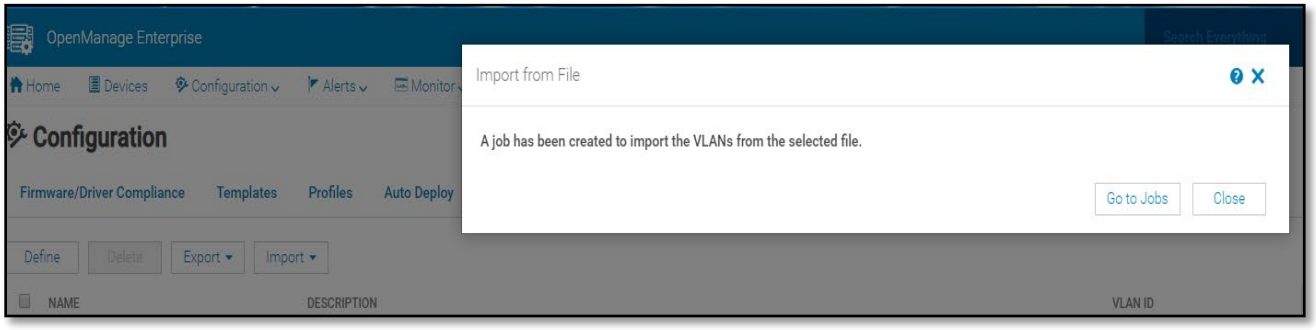

Figure 20 Easier OME-M workflows: Job created to import networks

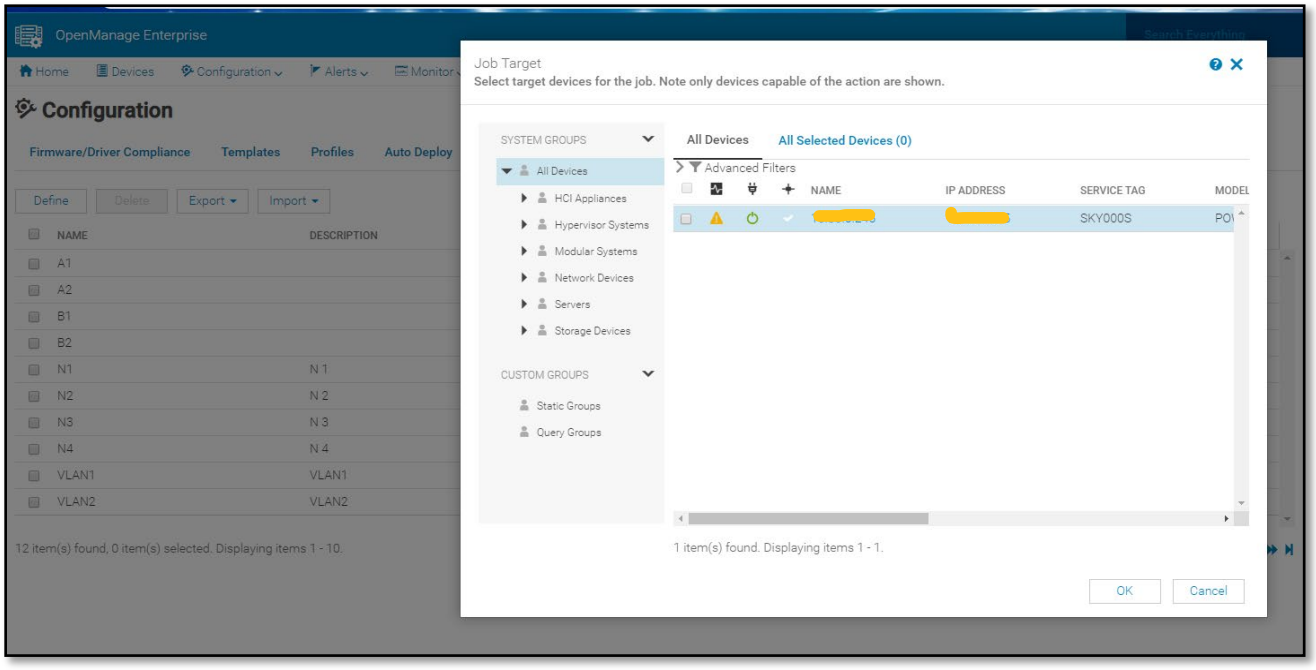

Figure 21 Easier OME-M workflows: Import VLANs from Chassis

An additional performance improvement include the ability to affect changes to VLAN assignment without server reboots. With OME 3.4, if changes to VLAN assignments to NIC ports in a template are made, the changes can be propagated to modular servers that the template had been previously deployed to without requiring a server reboot.

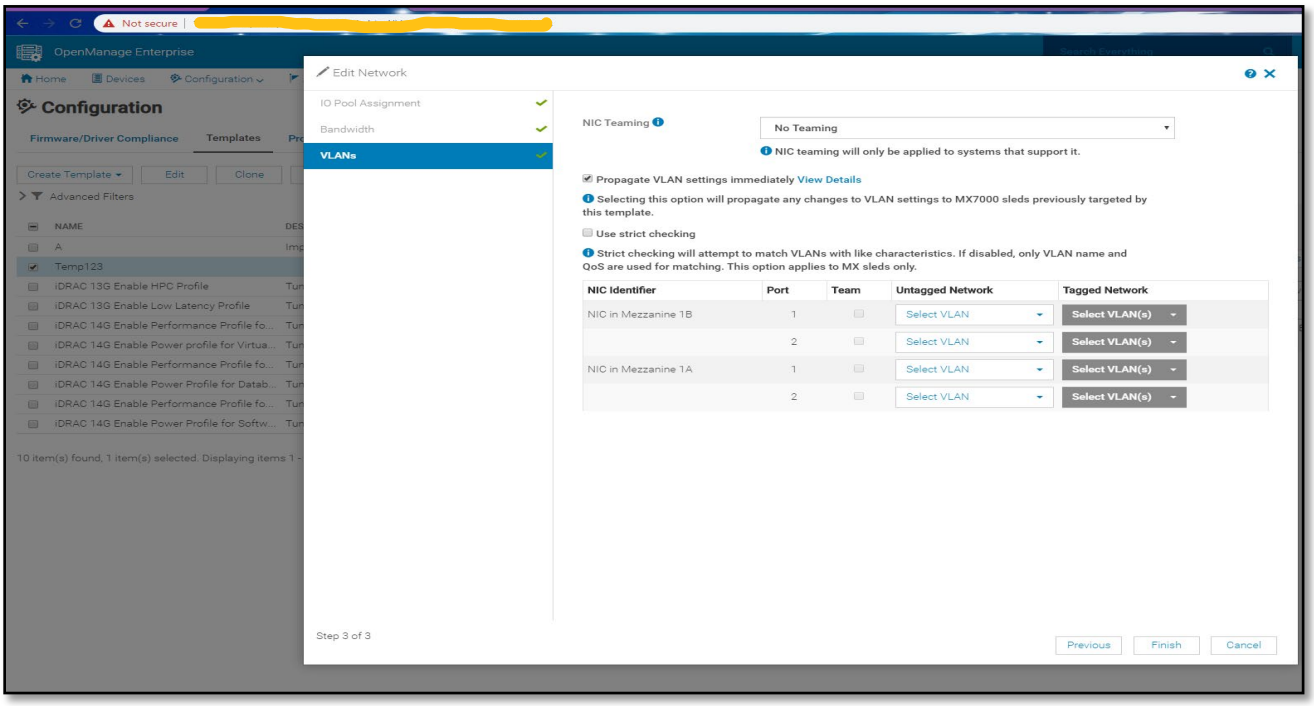

Figure 22 Easier OME-M workflows: VLAN assignment changes can be propagated to modular sleds in the NGM chassis, w/o a reboot of the sleds (Propagate checkbox).

The user can also specify if all parameters of VLANs should be matched (use strict checking) or simply best match (name and QoS only) should be used during propagation.

2.5 Troubleshooting issues

Symptom	What to check
Not all devices in the device picker can be targeted for profile deployment.	• Check if another profile is already deployed to the target that cannot be selected. For example, if a profile P1 is assigned to a device D1, another profile P2 cannot be assigned to D1, without unassigning P1 from D1. • Check task execution service logs.
Deployment cannot be configured successfully (no deployment job created).	• Check the application log for basic payload validation and task creation errors.
Deployment job is created but the deployment fails.	• Check the task execution service log for causes (specifically if there are attribute processing failures, connection errors, errors with identity assignment, and so on).

Symptom	What to check
	• If possible, the target device can also be checked for logs or job queue updates via the iDRAC UI.
Not all the VLANs are imported successfully.	• VLAN definitions that conflict with existing VLAN definitions in OME cannot be imported. The VLAN import job execution history provides details on the VLANs that were successfully imported or those that failed to import.

A.1 Related resources

OpenManage Enterprise Version 3.4 and OpenManage Enterprise - Modular Edition Version 1.20.00 RESTful API Guide:: https://topics-cdn.dell.com/pdf/dell-openmanage-enterprise_api-guide5_en-us.pdf