DELL Technologies

Technical Whitepaper

Scope Based Access Control with OpenManage Enterprise 3.6

Abstract

With OME 3.6, scope restriction for Device Managers is possible. A scope restricted user only sees what belongs to them. Read on for details.

August 2021

Revisions

Date	Description
August 2021	Initial release

Acknowledgements

Authored by: OpenManage Enterprise (OME) Engineering

Pushkala Iyer, Reg Stumpe, Gabe Stern

Table of contents

Revisions....1

Acknowledgements....1

Table of contents....3

Executive summary....4

1 Scope Based Access Control....5

1.1 What is Scope Based Access Control?....5

1.2 Assigning Scope....5

1.3 Restricted View....8

1.4 Transfer of Ownership....14

A.1 Related resources....15

Executive summary

OpenManage Enterprise has built-in Role Based Access Control, with three built-in roles – Administrator, Device Manager, and Viewer. Each role differs in the privileges the role has. In OME 3.6 and later, Scope Based Access Control is implemented. This feature enables an Administrator to restrict the scope of a Device Manager user to one or more groups. Read on to understand how SBAC can be enforced with OME and what a scope restricted user sees.

1 Scope Based Access Control

This technical whitepaper describes the new Scope Based Access Control feature implemented in OME 3.6 and how it can be used to limit what a user sees.

1.1 What is Scope Based Access Control?

The reader is likely familiar with **R**ole **B**ased **A**ccess **C**ontrol (**RBAC**) built into OME. With RBAC, there are built-in (pre-defined) roles, with specific sets of privileges for each role. OME comes with three built-in roles: the Administrator, Device Manager, and Viewer.

While RBAC distinguishes what users of a particular role can do vs. users of another role, it does not discriminate on the targets of an action. In other words, Administrators, Device Managers, and Viewers are restricted by privileges as to what actions they can perform, but they are not limited to which devices or groups they can perform actions.

This is where **S**cope **B**ased **A**ccess **C**ontrol (**SBAC**) comes in.

With SBAC, an administrator can restrict a Device Manager role to a set of device groups which constitutes their scope. This means that for a scope restricted Device Manager user, the privileges enabled by their role can only be exercised against their allocated scope, the specific set of device groups. A scope restricted Device Manager only sees content relevant to them in the UI, no other content is displayed. Scope restriction is only available for the Device Manager role.

To summarize:

- Administrators can see and act on all devices / groups in the console.
- Viewers are read only users, who can see all devices / groups in the console.
- Device Managers, if scope restricted, can only see, and perform actions on devices / groups / other entities in their scope.

1.2 Assigning Scope

Administrators can restrict the scope of Device Managers by assigning specific scope to them. Scope assignment can be done while creating the Device Manager user or at a later point of time, by editing the Device Manager user. For easy understanding, UI screens are included below.

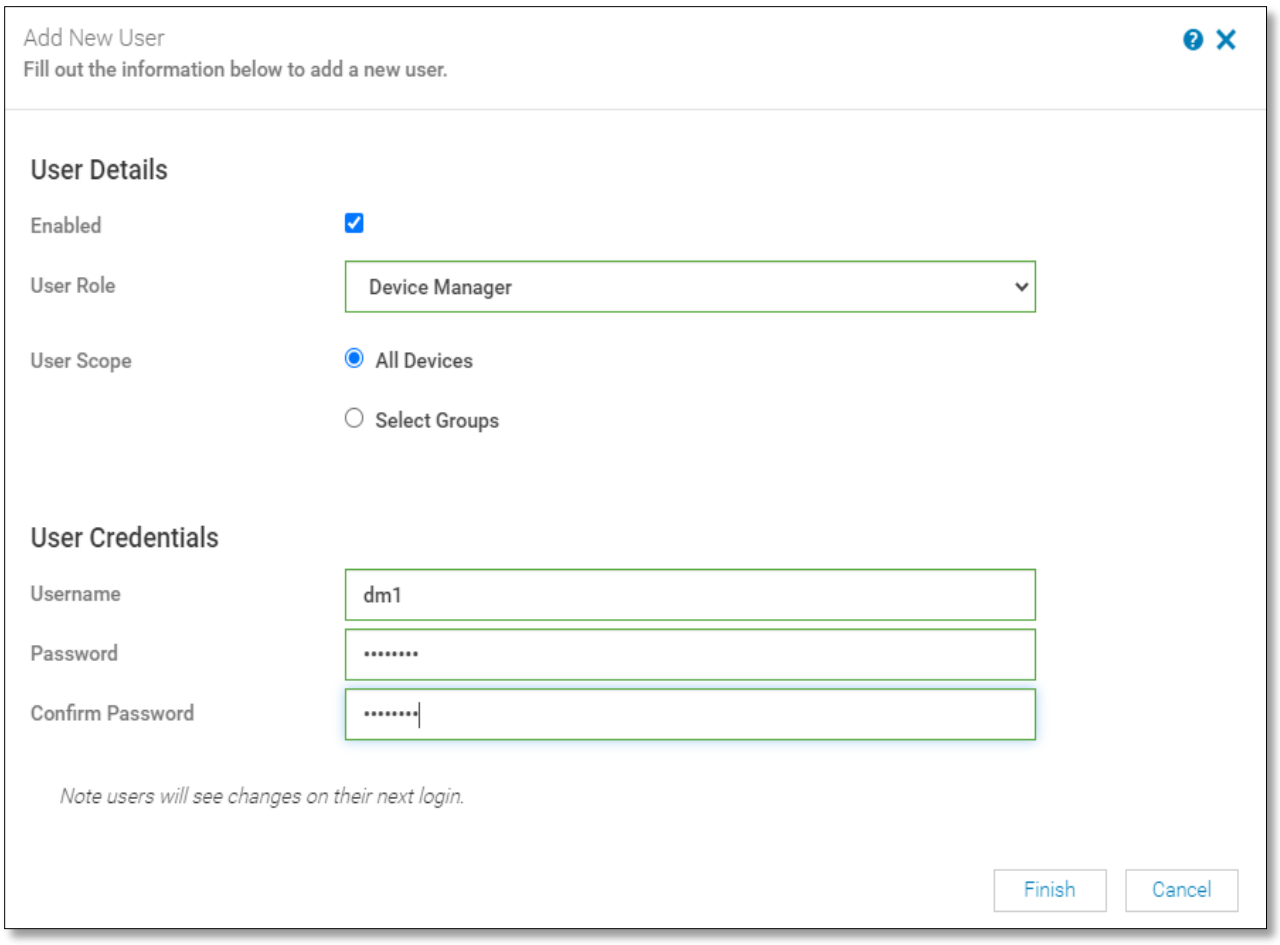

Figure 1 Administrator creates a new Device Manager user. By default, scope is unrestricted – set to “All Devices”.

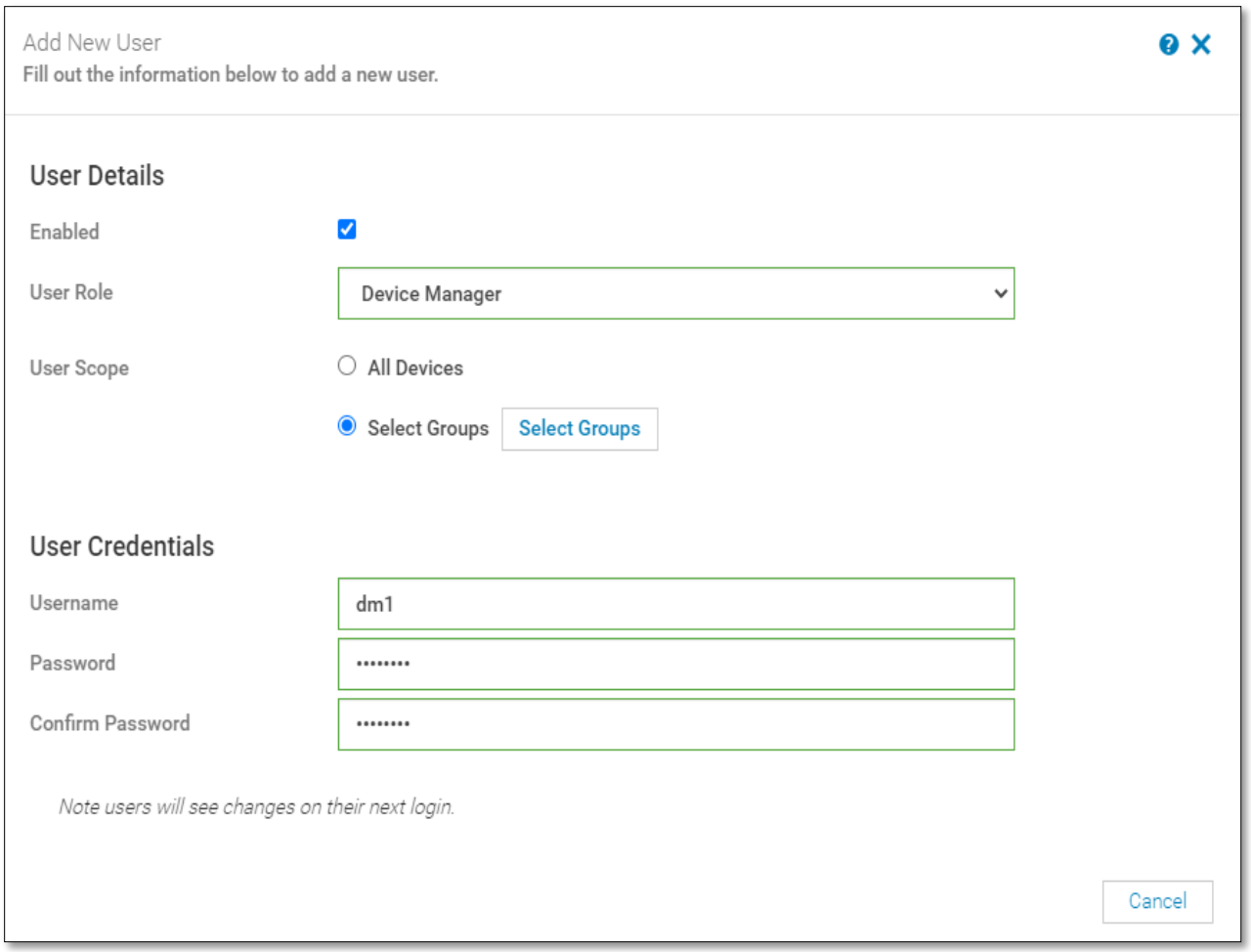

Figure 2 The Administrator can “scope restrict” the Device Manager by clicking **Select Groups** and then selecting one or more groups.

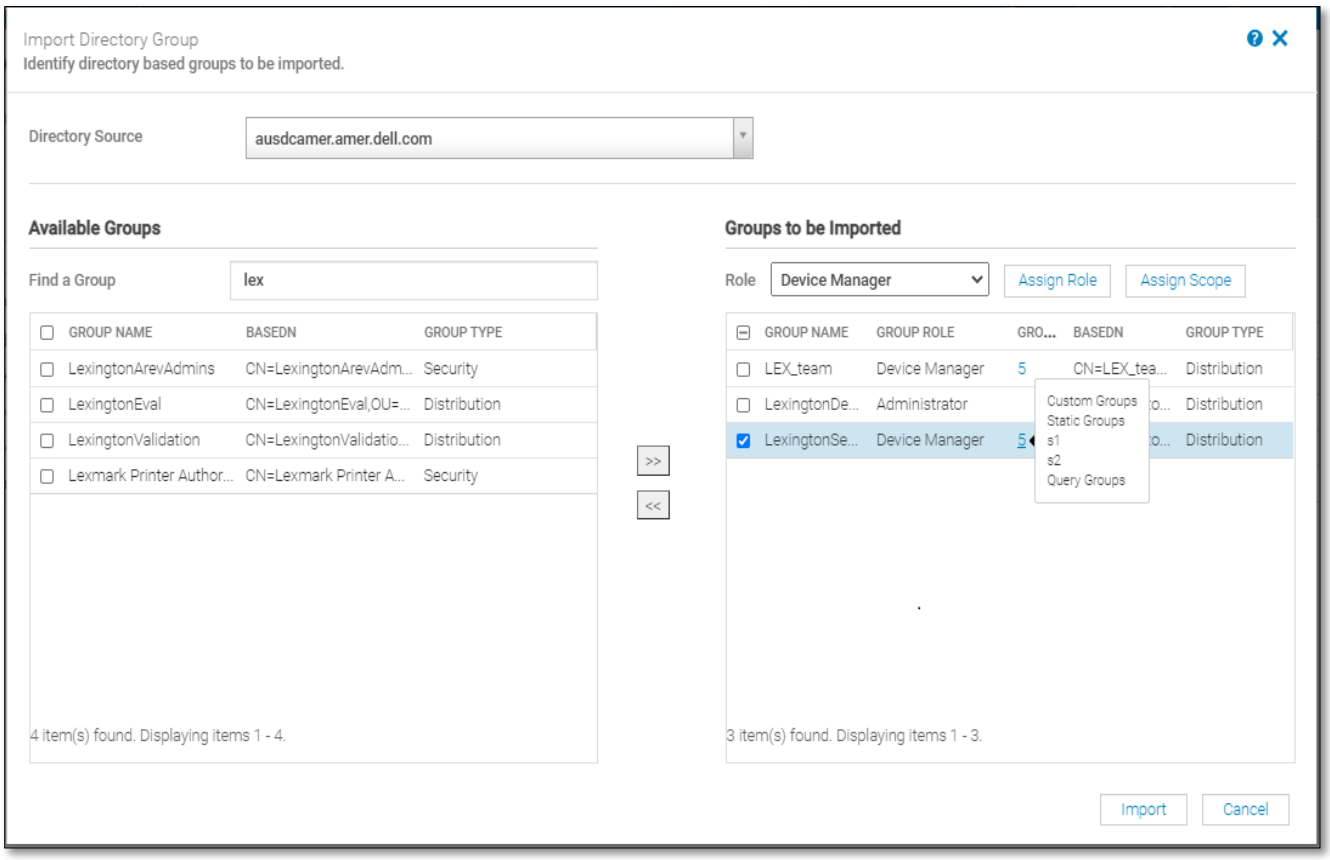

Figure 3 Scope restriction for directory users – once a directory group has been assigned to Device Manager role, access can be restricted to one or more groups as shown via the **Assign Scope** button.

1.3 Restricted View

An additional feature that is a natural outcome of SBAC functionality is Restricted View.

In particular, Device Managers will only see the following:

- Groups (therefore, devices in those groups) in their scope.
- Entities that they own (such as Jobs, Alert Policies, Profiles, and so on)
- Community entities (such as Identity Pools and VLANs – these entities can be used by everyone accessing the console and do not need to be restricted to specific users).
- Built-in entities of any kind.

If Device Managers scope is unrestricted, then they can see All Devices and all groups / devices, but they can only see their own entities for items such as Jobs, Alert Policies, Baselines, and so on. They would continue to see any community entities and built-in entities of any kind.

For directory users, what a scope restricted user sees depends on the directory groups they are a member of.

If a user is a member of multiple directory groups, each with the Device Manager Role and each directory group has distinct scope assignments then the user's scope is the union of the scopes of those directory groups.

Examples:

1. User dm1 is a member of 2 AD groups (RR5-Floor1-LabAdmins, RR5-Floor3-LabAdmins). Both AD groups have been assigned the Device Manager role, with scope assignments for the AD groups are as follows: RR5-Floor1-LabAdmins is assigned ptlab-servers, RR5-Floor3-LabAdmins is assigned smdlab-servers. Now the scope of the Device Manager dm1 is the union of ptlab-servers and smdlab-servers.

2. User dm1 is a member of 2 AD groups (adg1, adg2). Both AD groups have been assigned the Device Manager role, with scope assignments for the AD groups as follows: adg1 is given access to g1, adg2 is given access to g2. If g1 is the superset of g2, then the scope of dm1 is the larger scope (g1, all its child groups, and all leaf devices). If g1 and g2 are disjoint groups, the scope of dm1 is now the union of g1 and g2.

When a user is a member of multiple AD groups that have different roles, the higher-functionality role takes precedence (in the order Administrator, Device Manager, Viewer).

3. User user1 is a member of 2 AD groups (adg1, adg2). The AD group adg1 has Administrator role, but adg2 is assigned a Device Manager role scoped to g1. By virtue of being a member of both adg1 and adg2, user1 is now an Administrator on the console.

Screenshots will illustrate what a scope restricted Device Manager user sees.

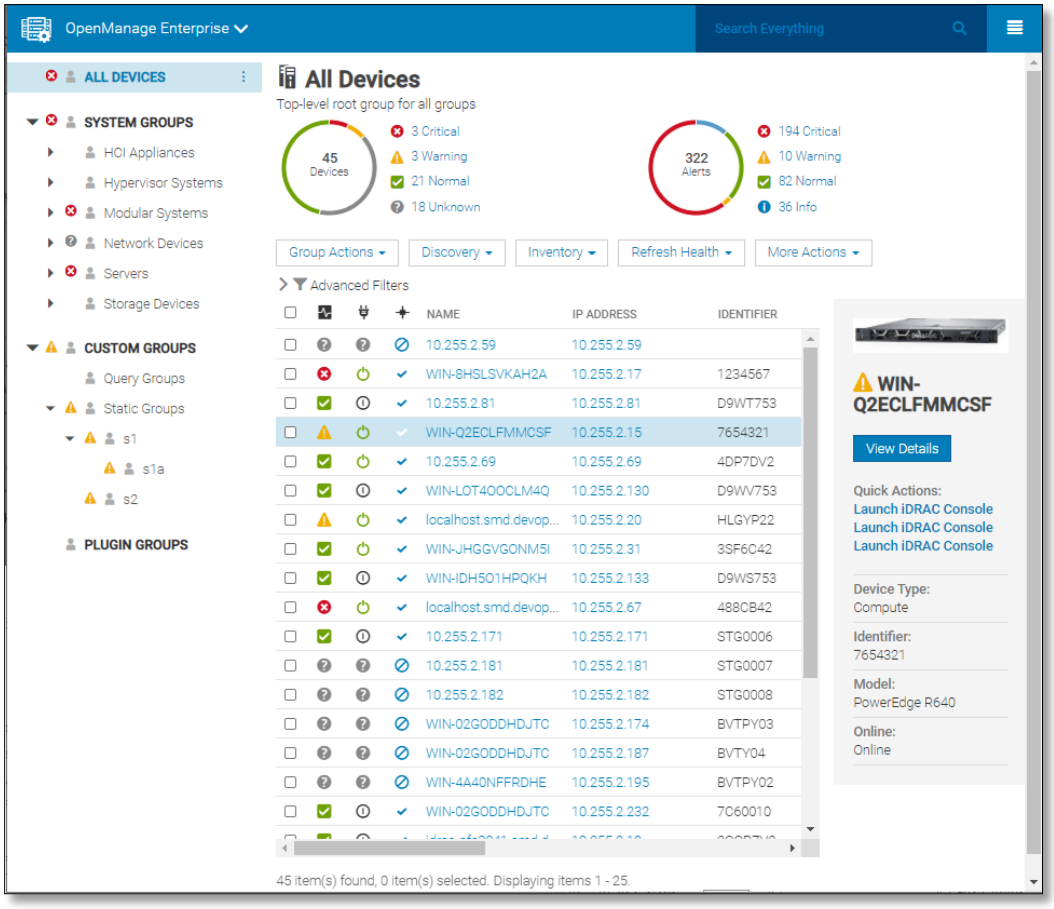

Figure 4 New “All Devices” view – unrestricted for Administrator users

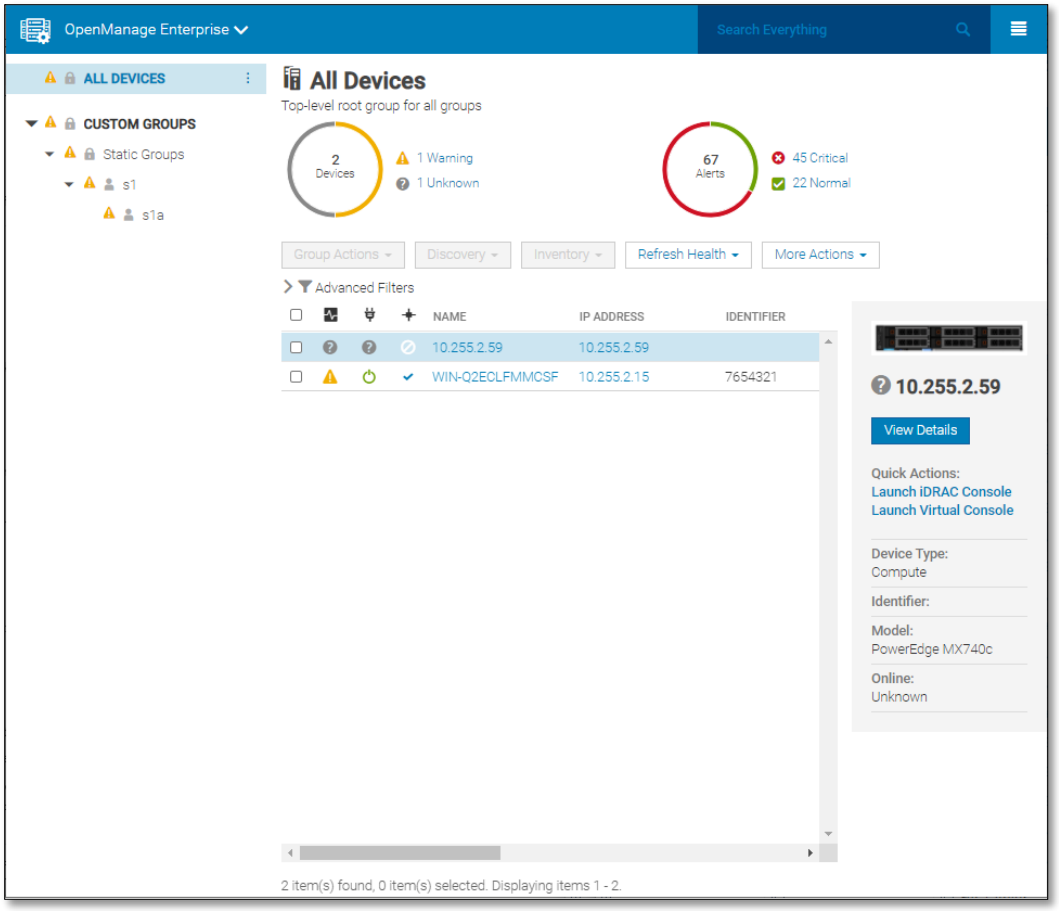

Figure 5 “All Devices” view for a Device Manager user, whose scope is restricted to a static group, s1.

Other than devices and groups, there are multiple other kinds of entities in the console such as Alert Policies, Jobs, Baselines and so on. The table below lists the different pages in OME, and what should be expected for a scope restricted Device Manager. Pages with actions (such as Discovery or Application Settings) that are not available to a Device Manager are not listed.

Page / Portal	**Any change for a scoped DM?**	**Details**
Home Portal	Yes	The group picker displays the “All Devices” root group. The various home portal donuts and widgets display data corresponding to the user’s scope.
All Devices	Yes	There is a change in the Tree hierarchy, with a new single root group – “All Devices”. The LHS tree controls visually indicate operational access.

		The user will see the hierarchy from “All Devices” to the groups that have been granted to the Device Manager. The Device Manager will not see the hierarchy from “All Devices” to other built-in / custom / plugin groups, to which access has not been granted.
Configuration: Firmware (FW) / Driver compliance: Catalog Management	No changes.	FW Catalogs are treated as community entities.
Configuration: FW / Driver compliance: Baselines	Yes.	Device Managers can see only the baselines that they own. Target Picker only shows FW update capable devices / groups that are in the Device Manager’s scope.
Configuration: FW / Driver compliance: Compliance Report	No changes.	Given a set of targets, the update should only run for those targets that are in the Device Manager’s scope. The targets are evaluated for scope when the update job runs.
Configuration: Templates	Yes.	Device Managers can see only the built-in templates and templates that they own. Only “Clone” and “Export” are allowed on built-in templates. The target picker only shows “Deploy capable” devices / groups that are in the Device Manager’s scope.
Configuration: Profiles	Yes.	Device Managers can see only the profiles that they own. Target Picker only shows “Deploy capable” devices that are in the Device Manager’s scope.

Configuration: Configuration compliance: Template Management	Yes.	Device Managers can see only the compliance templates they own.
Configuration: Configuration Compliance: Baselines	Yes.	Device Managers can see only the compliance baselines they own.
Configuration: Configuration Compliance: Compliance Report	No changes.	Given a set of targets, make compliant should only run for those targets that are in the Device Manager's scope.
Configuration: Identity Pools	Minor changes.	Identity pools are treated as community entities. Pool usage counts reflect total usage from pools. The grid shows the usage details as applicable to the Device Manager's scope. (i.e., if there are devices outside the Device Manager's scope that are using virtual identities from an identity pool, that usage info will not be shown in the grid).
Configuration: VLANs	No changes.	VLANs are treated as community entities.
Alerts: Alert Log	Yes.	Device Managers can see only the alerts from devices in their scope, any appliance alerts and any alerts from un-discovered devices.
Alerts: Alert Policies	Yes.	Device Managers can see only the built-in alert policies and any alert policies they own. "Edit / Enable / Disable / Delete" are not allowed for built-in policies. Target Picker only shows devices / groups that are in the Device Manager's scope.
Monitor: Audit Logs	No changes.	Device Managers can see all activity on the console.
Monitor: Jobs	Yes.	Device Managers can see built-in jobs and jobs that they own. "Enable / Disable / Delete" are not allowed for built-in jobs. When any job runs, it

		only runs on the targets in that Device Manager's scope.
Monitor: Warranty	Yes.	Device Managers see only the Warranty information from Devices in their scope.
Monitor: Reports	Yes.	Device Managers see built-in Reports and any reports they own. "Edit / Copy / Delete" are not available for built-in reports. When any report is run, the results are pertinent to the user's scope / ownership.
Global Search	Yes.	Search results are pertinent to the user's scope / ownership.

Table 1: OME pages and effects for a scope restricted Device Manager.

1.4 Transfer of Ownership

This is a new workflow and is intended to be used when a Device Manager leaves the organization. The entities that the Device Manager owns or owned can be transferred to their replacement Device Manager for continued operational ease. The screenshots below illustrate the workflow.

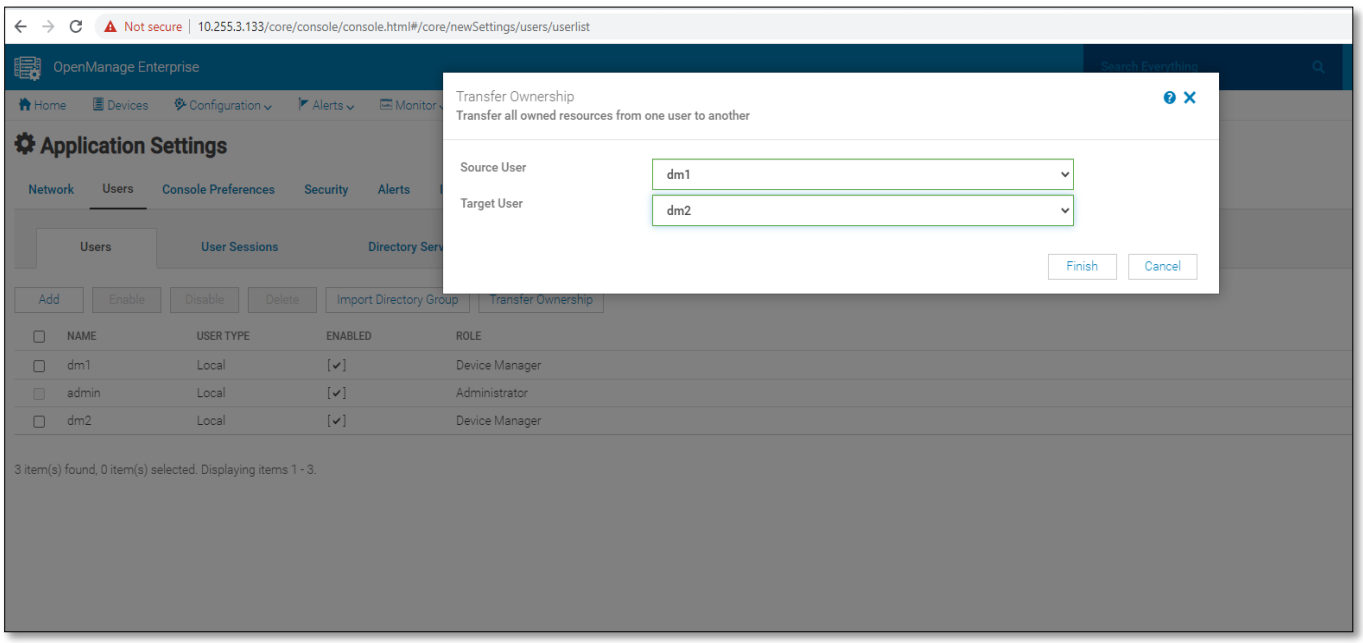

Figure 6 Picking source and target users for transfer of ownership.

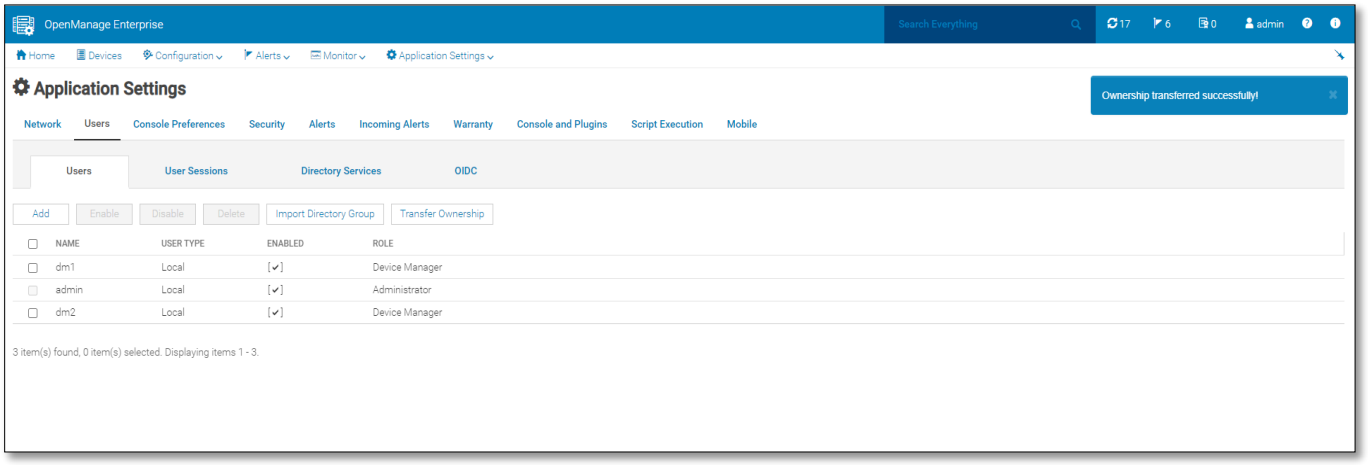

Figure 7 Confirmation that entities have been successfully transferred.

If Device Managers do not own any entities, then Transfer of Ownership does not apply to them (they cannot be chosen for a source user in Figure 6).

A.1 Related resources

OME 3.6 API Guide : Dell Technologies Developer Portal.

OME 3.6 User's Guide : OME support sites