

Dell EMC OpenManage Essentials Version 2.5

User's Guide

Notes, cautions, and warnings



NOTE: A NOTE indicates important information that helps you make better use of your product.



CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1 About OpenManage Essentials.....	19
New in this release.....	19
Other information you may need.....	19
Contacting Dell.....	20
2 Installing OpenManage Essentials.....	21
Installation prerequisites and minimum requirements.....	21
Terms and conditions for using Relational Database Management Systems.....	21
Minimum login roles for Microsoft SQL Server.....	22
Recommended database size.....	22
Download OpenManage Essentials.....	23
Installing OpenManage Essentials.....	23
Custom Setup Installation.....	25
Setting up OpenManage Essentials Database on a Remote SQL Server.....	25
Retargeting the OpenManage Essentials Database.....	26
Backing up the OpenManage Essentials Database.....	26
Restoring the OpenManage Essentials Database.....	26
Creating a new user in SQL Server.....	27
Connecting to the OpenManage Essentials Database.....	27
Installing OpenManage Essentials on a domain controller.....	28
Installing OpenManage Essentials on a domain controller with a remote database.....	28
Installing OpenManage Essentials on a domain controller with a local database	29
Adding users to the OpenManage Essentials user groups.....	30
Enabling SQL Server and Windows Authentication Mode in SQL Server	30
Verifying SQL Server TCP or IP Status	31
Installing SupportAssist Enterprise.....	31
Installing Repository Manager.....	32
Installing License Manager.....	32
Upgrading OpenManage Essentials.....	33
Reconfiguring OpenManage Essentials version 2.5 after upgrading.....	34
Uninstalling OpenManage Essentials.....	35
Migrating IT Assistant to OpenManage Essentials.....	36
3 Getting started with OpenManage Essentials.....	37
Launching OpenManage Essentials.....	37
Configuring OpenManage Essentials.....	37
Configuring the Discovery Wizard.....	38
Configuring Discovery Settings.....	38
Using the OpenManage Essentials Home Portal.....	39
OpenManage Essentials Heading Banner.....	40
Customizing the portals.....	40
Displaying additional reports and graphs.....	41

Drilling down charts and reports for more information.....	41
Saving and loading the portal layout.....	42
Updating the portal data.....	42
Hiding graphs and reports—Components.....	42
Rearranging or resizing graphs and reports—Components.....	43
Filtering data.....	43
Using the Search Bar.....	43
Searching items.....	44
Using the search drop-down list.....	44
Search results and the default actions.....	44
Map View—Home Portal.....	45
Viewing the user information.....	45
Logging in as a different user.....	45
Using the Update Available Notification Icon.....	46
Using the Warranty Scoreboard Notification Icon.....	46

4 OpenManage Essentials Home Portal — Reference..... 47

Dashboard.....	47
Home Portal Reports.....	47
Device by Status.....	48
Alerts by Severity.....	48
Discovered Versus Inventoried Devices.....	48
Task Status.....	49
Schedule View.....	49
Schedule View Settings.....	49
Device Warranty Report.....	50
Map View Interface—Home Portal.....	51

5 Discovering and inventorying devices.....52

Supported devices, protocols, and features matrix—SNMP, WMI, and WS-Man.....	52
Supported devices, protocols, and features matrix—IPMI, CLI, and SSH.....	56
Supported storage devices, protocols, and features matrix.....	58
Setting up and configuring VMware ESXi 5.....	59
Legend and definitions.....	60
Using the Discovery and Inventory Portal.....	60
Protocol support matrix for discovery.....	61
Protocol support matrix for system update.....	62
Devices not reporting Service Tag.....	62
Creating a discovery and inventory task.....	63
Changing the default SNMP port.....	64
Discovering and inventorying devices by using WS-Man or REST protocol with a root certificate.....	65
Discovering a chassis and its components by using Guided Wizard.....	66
Excluding ranges.....	67
Viewing configured discovery and inventory ranges.....	67
Scheduling discovery.....	67
Discovery Speed Slider.....	68

Multithreading.....	68
Scheduling inventory.....	68
Configuring status polling frequency.....	69
Task pop-up notifications.....	69
Configuring task pop-up notifications.....	70
Enabling or disabling task pop-up notifications.....	70

6 Discovery And Inventory — Reference..... 71

Discovery and Inventory Portal Page Options.....	71
Discovery and Inventory Portal.....	71
Last Discovery and Inventory.....	71
Discovered Versus Inventoried Devices.....	72
Task Status.....	72
Viewing Device Summary.....	73
Viewing Device Summary Filter Options.....	73
Add Discovery Range.....	74
Discovery Configuration.....	74
Discovery Configuration Options.....	74
Device Type Filtering.....	75
ICMP Configuration.....	76
ICMP Configuration Options.....	76
SNMP Configuration.....	76
SNMP Configuration Options.....	77
WMI Configuration.....	78
WMI Configuration Options.....	78
Storage Configuration.....	78
Storage Configuration Options.....	78
WS-Man Configuration.....	78
WS-Man Configuration Options.....	79
REST configuration.....	79
REST configuration options.....	80
SSH Configuration.....	80
SSH Configuration Options.....	80
IPMI Configuration.....	81
IPMI Configuration Options.....	81
Discovery Range Action.....	81
Summary.....	82
Add Exclude Range.....	82
Add Exclude Range Options.....	82
Discovery Schedule.....	82
Viewing Discovery Configuration.....	83
Discovery Schedule Settings.....	83
Inventory Schedule.....	84
Inventory Schedule Settings.....	84
Status Schedule.....	84
Status Polling Schedule Settings.....	84

Discovery Ranges.....	85
Exclude Ranges.....	85

7 Managing devices.....86

Viewing devices.....	86
Device Summary Page.....	86
Nodes and symbols description.....	88
Device details.....	88
Viewing device inventory.....	89
Viewing alerts summary.....	90
Viewing noncompliant devices associated with a catalog baseline.....	90
Viewing noncompliant devices associated with a configuration baseline.....	90
Viewing System Event Logs.....	90
Searching for Devices.....	90
Creating a New Group.....	91
Adding Devices to a New Group.....	91
Adding Devices to an Existing Group.....	92
Hiding a Group.....	92
Deleting a Group.....	92
Associating a catalog baseline to custom device groups.....	92
Disassociating a catalog baseline from custom device groups.....	93
Single Sign-On.....	93
Creating a Custom URL.....	93
Launching the Custom URL.....	93
Configuring Warranty Email Notifications.....	94
Configuring Warranty Scoreboard Notifications.....	94
Configuring Warranty Pop-Up Notifications.....	95
Configuring Warranty Update Settings.....	95
Using Map View.....	95
Map Providers.....	97
Configuring Map Settings.....	98
General Navigation and Zooming.....	98
Home View.....	99
Tool Tip.....	99
Selecting a Device on Map View.....	99
Health and Connection Status.....	99
Multiple Devices at the Same Location.....	100
Setting a Home View.....	100
Viewing All Map Locations.....	101
Adding a Device to the Map.....	101
Moving a Device Location Using the Edit Location Details Option.....	101
Importing Licensed Devices.....	102
Using the Map View Search Bar.....	103
Removing All Map Locations.....	104
Editing a Map Location.....	105
Removing a Map Location.....	105

Exporting All Device Locations.....	105
PowerEdge FX Chassis View.....	106
Tool Tip and Device Selection.....	106
Overlays.....	107
Right-Click Actions.....	107
Navigation Trail.....	107
Support For PowerEdge FX Chassis Sleds.....	108
VLAN Configuration Management.....	108
Requirements for VLAN Configuration Management.....	108
Viewing the VLAN Configuration Inventory.....	109
Assigning VLAN IDs.....	109
Resetting all VLAN IDs.....	110
Setting the Default VLAN ID Values.....	110
Dell NAS Appliance Support.....	110
OEM Device Support.....	111

8 Devices — Reference..... 112

Viewing Inventory.....	112
Viewing Alerts.....	112
Viewing Hardware Logs.....	113
Hardware Log Details.....	113
VLAN Configuration.....	113
VLAN Configuration Task.....	114
Task Results.....	115
Alert Filters.....	116
Viewing noncompliant systems—Devices	116
Non-Compliant Firmware and Drivers.....	116
Non-Compliant Configurations.....	117
Device Search.....	117
Query Results.....	118
Creating Device Group.....	118
Device Group Configuration.....	119
Device Selection.....	119
Summary — Group Configuration.....	120
Map View Interface—Devices Tab.....	120
Devices at this location.....	121
Map Settings.....	121

9 Deployment and reprovisioning..... 123

Server Configuration Management license.....	124
Licensable servers.....	124
Purchasing license.....	124
Deploying the license.....	124
Verifying license information.....	124
Viewing unlicensed server targets.....	125
Device requirements for deployment and compliance tasks.....	125

Getting started for device configuration deployment.....	126
Viewing the Deployment Portal.....	126
Configuring the deployment file share.....	126
Adding devices to repurpose and bare-metal devices group.....	127
Overview of bare-metal deployment.....	127
Creating a device deployment template.....	128
Creating a device deployment template from a device configuration file.....	128
Creating a device deployment template from a reference device.....	129
Managing device deployment templates.....	130
Viewing device deployment template attributes.....	130
Cloning a device deployment template.....	130
Editing a device deployment template.....	131
Exporting a device deployment template.....	132
Deploying a device deployment template—Bare-metal deployment.....	132
Creating a chassis deployment template from a chassis.....	134
Managing chassis deployment templates.....	135
Viewing and editing chassis deployment template attributes.....	136
Exporting a chassis deployment template.....	136
Cloning a chassis deployment template.....	136
Deploying a chassis infrastructure template.....	136
Deploying IOA configuration template.....	138
IOA operational modes and the deployment task status.....	140
Deploying a network ISO image.....	140
Removing devices from the repurpose and bare-metal devices group.....	141
Auto deploying device configurations.....	141
Configuring Auto Deployment Settings.....	142
Setting up device configuration auto deployment—Bare-metal deployment.....	142
Managing Auto Deployment Credentials.....	144
Adding a Discovery Range for Auto Deployment.....	145
Removing Devices From an Auto Deployment Task.....	145
Importing Device Specific Attributes.....	146
Import File Requirements.....	146
Exporting Device Specific Attributes.....	146
Viewing the Deployment Tasks.....	147
Managing the Virtual Input-Output Identities of a Server—Stateless Deployment.....	147
Overview of Stateless Deployment.....	147
Virtual Input-Output Pools.....	148
Creating a Virtual Input-Output Pool.....	148
Editing a Virtual Input-Output Pool.....	151
Viewing the Definitions of a Virtual Input-Output Pool	151
Renaming a Virtual Input-Output Pool.....	152
Deleting a Virtual Input-Output Pool.....	152
Viewing the Virtual Input-Output Identities Assigned or Deployed on a Device.....	152
Compute Pools.....	153
Creating a Compute Pool.....	153

Deploying a device configuration template—Stateless deployment.....	154
Automatic Locking of a Compute Pool.....	156
Unlocking a Compute Pool.....	157
Editing the Definitions of a Compute Pool.....	157
Viewing the Definitions of a Compute Pool	157
Removing a Server From a Compute Pool.....	158
Renaming a Compute Pool.....	158
Deleting a Compute Pool.....	158
Replacing a Server.....	158
Reclaiming Deployed Virtual Input-Output Identities of a Server.....	160
Reclaiming Assigned Virtual Input-Output Identities.....	160
Setting up device configuration auto deployment—Stateless deployment.....	161
Viewing device profiles.....	163
Known limitations for stateless deployment.....	163
Additional information.....	163

10 Deployment—Reference..... 165

Icons and descriptions.....	166
Repurpose and Bare Metal Devices.....	167
Auto Deployment.....	168
Tasks.....	168
Task Execution History.....	169
Device Configuration Template Details.....	169
IOA VLAN Attributes.....	170
Device Configuration Setup Wizard.....	171
File Share Settings.....	171
Add devices to repurpose and bare-metal devices group.....	171
Add Network.....	171
Network Types.....	172
Create Template Wizard.....	172
Create Virtual Input-Output Pool Wizard.....	173
Name and Description.....	173
Ethernet Identities.....	173
FCoE Node Name Identities.....	174
FCoE Port Name Identities.....	174
iSCSI IQN Identities.....	175
Summary.....	175
Virtual Input-Output Pools.....	176
Virtual Input-Output Pool Summary.....	176
Summary.....	177
Devices with Identities.....	177
Create Compute Pool Wizard.....	178
Name and Description.....	178
Select Template.....	178
Select ISO Location.....	178
Select Virtual Input-Output Pool.....	179

Select Devices.....	179
Edit Attributes.....	179
Summary.....	184
Compute Pool Summary.....	184
Compute Pool Details.....	185
Server Details.....	185
Deploy Template Wizard.....	186
Name and Deploy Options.....	186
Select Template.....	186
Select Devices.....	187
Select ISO Location.....	187
Select Virtual Input-Output Pool.....	188
Edit Attributes.....	188
Options.....	192
Set Schedule.....	193
Preview.....	193
Summary.....	194
Setup Auto Deployment Wizard.....	195
Select Deploy Options.....	195
Select Template.....	195
Select ISO Location.....	196
Select Virtual Input-Output Pool.....	196
Import Service Tags or Node IDs.....	197
Edit Attributes.....	197
Execution Credentials.....	201
Summary.....	203
Manage Auto Deployment Credentials.....	203
Credentials.....	203
Devices.....	204
Replace Server Wizard.....	204
Name.....	204
Source and Target.....	205
Review Source Attributes.....	205
Options.....	207
Credentials.....	208
Summary.....	208
Reclaim Identities Wizard.....	209
Name.....	209
Select Devices.....	209
Identity Assignments.....	210
Options.....	210
Credentials.....	211
Summary.....	211

11 Managing device configuration baseline..... 212

Viewing the Device Compliance Portal.....	212
---	-----

Getting started for device configuration compliance.....	212
Device configuration compliance overview.....	213
Configuring the credentials and device configuration inventory schedule.....	213
Viewing the device configuration inventory.....	214
Creating a device compliance baseline for servers and chassis.....	214
Associating target devices with a baseline.....	215
Viewing compliance status of devices.....	215
Remediating noncompliant devices.....	216
Viewing compliance tasks.....	216
Viewing server backup profiles.....	217
Replacing a server from backup profile.....	217
12 Configuration – Reference.....	219
Device Compliance.....	220
Device Compliance Graph.....	220
Device Compliance Table.....	220
Tasks.....	220
Task Execution History.....	221
Associate Devices To a Baseline Wizard.....	222
Select Baseline.....	222
Select Devices.....	222
Make Devices Compliant.....	222
Name.....	222
Select Devices.....	222
Options.....	223
Set Schedule.....	223
Summary.....	224
Configuration Inventory Schedule Wizard.....	224
Inventory Credentials.....	224
Schedule.....	225
Backed-Up Devices.....	225
Devices Table.....	225
Attributes Table.....	226
13 Viewing inventory reports.....	227
Choosing predefined reports.....	227
Predefined reports.....	227
Filtering report data.....	230
Exporting reports.....	230
14 Reports — Reference.....	231
Server Inventory Reports.....	231
Agent and Alert Summary.....	232
Agent Health Status.....	233
Server Overview.....	233
Field Replaceable Unit Information.....	234

Hard Drive Information.....	234
iDRAC Performance Minimum or Maximum.....	235
iDRAC Performance Average or Peak.....	236
Memory Information.....	236
Modular Enclosure Information.....	237
NIC Information.....	237
PCI Device Information.....	238
Processor Information.....	238
Storage Controller Information.....	239
Virtual Disk Information.....	239
Server Configuration Reports.....	239
Server Components and Versions.....	240
BIOS Configuration.....	240
iDRAC Network Configuration.....	241
Device Configuration Compliance.....	242
Baseline Association.....	242
Assigned Identity Attributes.....	242
All Identity Attributes.....	243
Warranty and License Reports.....	243
Warranty Information.....	244
License Information.....	244
Virtualization Reports.....	245
ESX Information.....	245
HyperV Information.....	245
Asset Reports.....	246
Asset Acquisition Information.....	246
Asset Maintenance Information.....	247
Asset Support Information.....	248
Device Location Information.....	248

15 Viewing warranty reports.....250

Extending warranty.....	250
-------------------------	-----

16 Managing alerts.....251

Viewing alerts and alert categories.....	251
Viewing alert logs.....	251
Understanding alert types.....	251
Viewing internal alerts.....	252
Viewing alert categories.....	252
Viewing alert source details.....	252
Viewing previously configured alert actions.....	252
Viewing application launch alert action.....	252
Viewing email alert action.....	252
Viewing alert ignore action.....	253
Viewing alert trap forward action.....	253
Handling alerts.....	253

Flagging an alert.....	253
Creating and editing a new view.....	253
Configuring alert actions.....	253
Setting up email notifications.....	253
Ignoring alerts.....	254
Running a custom script.....	255
Forwarding alerts.....	255
Forwarding alerts use case scenarios.....	256
Working with sample alert action use cases.....	256
Use cases in alert actions.....	256
Configuring alert log settings.....	257
Renaming alert categories and alert sources.....	257
Alert pop-up notifications.....	257
Configuring alert pop-up notifications.....	258
Enabling or disabling alert pop-up notifications.....	258
Managing MIB files.....	258
About importing MIBs.....	259
Importing MIBs.....	260
Removing MIBs from OpenManage Essentials.....	260
Managing traps.....	260
Customizing trap definitions.....	260
Resetting built-in trap definitions.....	261
Configuring SNMPv3 traps.....	261

17 Alerts — Reference..... 263

Alert Logs.....	263
Predefined Alert View Filters.....	264
Alert Logs Fields.....	264
Alert Details.....	265
Alert Log Settings.....	265
Alert View Filters.....	266
Alert Filter Name.....	266
Severity.....	266
Acknowledgement.....	267
Summary — Alert View Filter.....	267
Alert Actions.....	267
Name and Description.....	268
Severity Association.....	268
Application Launch Configuration.....	268
E-Mail Configuration.....	270
Trap Forwarding.....	270
SNMP V3 Configuration.....	271
SNMP V3 Configuration Wizard.....	271
Category and Sources Association.....	272
Device Association.....	272
Date and Time Range.....	273

Alert Action — Duplicate Alert Correlation.....	273
Summary — Alert Action Details.....	273
Alert Categories.....	274
Alert Categories Options.....	274
Edit Trap Definitions.....	276
Alert Source.....	276
Manage MIBs.....	277
Manage MIBs Pane.....	277
Manage Traps Pane.....	277
Import MIB.....	277
Remove MIB.....	279
Troubleshooting MIB Import.....	279
Manage Traps.....	280
Custom Trap Definitions.....	280
Reset Built-in Trap Definitions.....	281

18 Updating BIOS, firmware, drivers, and system applications.....282

Viewing the System Update page.....	282
Understanding sources of system updates.....	283
Choosing the right source of system updates.....	283
Selecting an update catalog source.....	283
Viewing comparison results.....	284
Viewing compliant systems.....	284
Viewing noncompliant systems.....	284
Viewing non-inventoried systems.....	284
Viewing systems with issues and resolutions.....	284
Creating a catalog baseline.....	284
Viewing the Default Catalog.....	284
System Update Use Case Scenarios.....	285
Applying system updates by using the Non-Compliant Systems tab.....	287
Applying System Updates by using the System Update Task wizard.....	288
Viewing status of the System Update task.....	290
Updating systems without OpenManage Server Administrator.....	291
Issues and Resolutions Use Case Scenarios.....	291
Configuring automatic purging of downloaded system update files.....	291

19 System Update — Reference..... 292

Filter Options.....	293
System Update.....	293
Compliance Report.....	293
Compliant Systems.....	295
Non-Compliant Firmware and Drivers.....	295
System Update Task.....	296
Non-Inventoried Systems.....	298
Inventory Systems.....	298
All System Update Tasks.....	298

Issues and Resolutions.....	298
Task Execution History.....	299
Select a Catalog Source.....	299
Dell Update Package.....	300
OpenManage Server Update Utility.....	300
Repository Manager.....	300
Viewing the Default Catalog.....	300
View MX Chassis Default Catalog.....	301
View Catalog Baseline Associations.....	301
List of Catalog Baselines.....	301
Create Catalog Baseline wizard.....	301
Baseline Details.....	302

20 Managing remote tasks..... 303

About remote tasks.....	303
Managing command line tasks.....	303
Managing RACADM command line tasks.....	304
Managing generic command line tasks.....	304
Managing server power options.....	306
Deploying OpenManage Server Administrator.....	306
Supported Windows and Linux Packages.....	307
Arguments.....	308
Deploying iDRAC Service Module.....	308
Supported Windows and Linux Packages.....	309
Collecting Firmware and Driver Inventory.....	310
Updating the inventory collector component.....	311
Working With Sample Remote Tasks Use Cases.....	311
Use Cases in Remote Tasks.....	312
Device Capability Matrix.....	313

21 Remote Tasks — Reference..... 316

Remote Tasks Home.....	316
Remote Tasks	317
All Tasks.....	317
Task Execution History.....	318
Server Power Options.....	318
Deployment Task.....	320
Command Line Task.....	322
Remote Server Administrator Command.....	322
Generic Command.....	324
IPMI Command.....	325
RACADM Command Line.....	326
Firmware and Driver Inventory Collection Task.....	328

22 Managing security settings..... 330

Using security roles and permissions.....	330
---	-----

Microsoft Windows authentication.....	331
Assigning user rights.....	331
Using Custom SSL Certificates—Optional.....	331
Configuring IIS Services.....	331
Supported protocols and ports in OpenManage Essentials.....	332
Supported protocols and ports on management stations.....	332
Supported protocols and ports on managed nodes.....	332
Supported Protocols and Ports on Management Stations.....	333
Supported Protocols and Ports on Managed Nodes.....	333
Dell EMC OpenManage Framework.....	334

23 Troubleshooting.....336

OpenManage Essentials Troubleshooting Tool.....	336
Troubleshooting Procedures.....	336
Troubleshooting Inventory.....	336
Troubleshooting Device Discovery.....	337
Troubleshooting Receiving SNMP Traps	337
Troubleshooting Discovery of Windows Server 2008–Based Servers.....	338
Troubleshooting SNMP Traps for ESX or ESXi Versions 3.5, 4.x, or 5.0.....	338
Troubleshooting Problems With Microsoft Internet Explorer.....	338
Troubleshooting Map View.....	339

24 Frequently Asked Questions.....340

Installation	340
Upgrade.....	340
Tasks.....	341
Optional Command Line Settings.....	341
Customization Parameters.....	342
MSI Return Code.....	343
E-mail Alert Action.....	344
Discovery.....	344
Inventory.....	347
System Update.....	348
Managing Device Configurations.....	349
Device Group Permissions.....	349
Device Group Permissions Portal.....	349
Remote and System Update Tasks.....	350
Custom Device Groups.....	350
Deployment and Configuration Compliance.....	350
Deployment and Configuration Compliance.....	350
Logs.....	351
Log Levels.....	352
Backup and Restore.....	352
Troubleshooting.....	352

25 Managing Device Group Permissions.....354

Adding Users to the OmeSiteAdministrators Role.....	354
Assigning Device Groups to a User.....	355
Removing Users From the OmeSiteAdministrators Role.....	355
26 OpenManage Mobile Settings.....	357
Enabling or Disabling Alert Notifications For OpenManage Mobile.....	357
Enabling or Disabling OpenManage Mobile Subscribers.....	357
Deleting an OpenManage Mobile Subscriber.....	358
Viewing the Alert Notification Service Status.....	358
Notification Service Status.....	358
Viewing the OpenManage Mobile Subscriber Information.....	359
Mobile Subscriber Information.....	359
Troubleshooting OpenManage Mobile.....	360
27 Settings — Reference.....	361
Alert Settings.....	361
Custom URL Settings.....	362
Deployment Settings.....	362
Device Tree Settings.....	363
Discovery Settings.....	363
Feature Usage Settings.....	364
Email Settings.....	364
General Settings.....	365
Task Settings.....	366
Warranty Notification Settings.....	366
Permissions.....	368
Common Tasks.....	368
Manage Device Group Permissions.....	368
Device Groups for Tasks and Patch Targeting.....	368
Purge Download Settings.....	368
28 Logs — Reference.....	370
User Interface Logs.....	370
Application Logs.....	370
29 Dell EMC Solutions.....	371
30 Right-Click Actions.....	372
Schedule View.....	372
Device Status.....	372
Associate Catalog Baseline.....	373
Discovery Range Summary.....	374
Managing Include Ranges.....	374
View Filters.....	374
Alerts.....	374
Remote Tasks.....	375

Custom URL	375
System Update Tasks.....	375
Attributes Tab.....	376
Templates.....	376
Compute Pools.....	376
Repurpose and Bare Metal	376
Compute Pool.....	376
Devices.....	377
Virtual Input-Output Pools.....	377
Virtual I/O Pool.....	377
Devices with Identities.....	377
Compliance by Template.....	378
Device Compliance.....	378

31 Tutorials..... 379

32 Using OpenManage Essentials Command Line Interface..... 380

Launching the OpenManage Essentials Command Line Interface.....	380
Creating an input file for Discovery Profile.....	380
Specifying IPs, ranges, or host names by using XML or CSV files.....	381
Specifying input files in PowerShell.....	381
Command Line Interface commands.....	381
Creating a discovery range.....	382
Editing a discovery range.....	382
Removing a discovery range.....	382
Creating a discovery range group.....	382
Editing a discovery range group.....	383
Removing a discovery range group.....	383
Enabling a discovery range or discovery range group.....	383
Disabling a discovery range or discovery range group.....	384
Creating a discovery exclude range.....	384
Removing a discovery exclude range.....	384
Running discovery, inventory, and status polling tasks.....	385
Removing devices	385
Retrieving the status execution progress of a discovery range.....	385
Stopping discovery range or group tasks.....	386
Creating a custom device group.....	386
Adding devices to a custom group.....	386
Deleting a custom device group.....	387

About OpenManage Essentials

OpenManage Essentials is a hardware management application that provides a comprehensive view of systems, devices, and components in the enterprise's network. With OpenManage Essentials, a web-based and one-to-many systems management application for systems and other devices, you can:

- Discover and inventory systems
- Monitor the health of systems
- View and manage system alerts
- Perform system updates and remote tasks
- View hardware inventory and compliance reports
- Deploy or reprovision a server, chassis, or an I/O Aggregator (IOA)
- Manage the configuration baseline of a server or chassis
- Manage the virtual I/O identity of a server

New in this release

- Support for the following features of a MX7000 chassis—as a standalone chassis and as a lead chassis in a Multi-Chassis Management (MCM) group:
 - Discovery, inventory, monitoring, and status polling
 - Alerts recognition and traps classification
 - System updates
 - Configuration template creation and deployment
 - Configuration compliance and remediation
 - Configuring VLANs on MX7000 chassis by using the blade server template deployment feature
- Support for the following devices:
 - Latest 14th generation PowerEdge servers including new blade servers of MX7000 chassis.
 - PowerEdge MX7000 modular enclosure
 - VxFlex Ready Nodes

For a complete list of supported device models, see the *Dell EMC OpenManage Essentials Support Matrix* at Dell.com/OpenManageManuals.

- Enhancement:
 - Enhanced view to display catalog baselines associated to the custom device groups.

Other information you may need

Table 1. Other information you may need

Document	Description	Availability
<i>Dell EMC OpenManage Essentials Support Matrix</i>	Lists the devices that are supported by OpenManage Essentials.	1. Visit Dell.com/OpenManageManuals . 2. Click OpenManage Essentials , and select the required version of OpenManage Essentials. 3. Click Manuals & documents to access these documents.
<i>Dell EMC OpenManage Essentials Readme</i>	Provides information about known issues and workarounds in OpenManage Essentials.	

Document	Description	Availability
<i>Dell EMC OpenManage Mobile User's Guide</i>	Provides information about installing and using the OpenManage Mobile application.	
<i>Dell EMC License Manager User's Guide</i>	Provides information about managing licenses and troubleshooting the License Manager.	
<i>Dell EMC Repository Manager User's Guide</i>	Provides information about using the Repository Manager to manage system updates.	
<i>Dell EMC OpenManage Essentials REST API Guide</i>	Provides information about integrating OpenManage Essentials using Representational State Transfer (REST) APIs and also includes examples of using REST APIs to perform common tasks.	Dell.com/OpenManageManuals or DellTechCenter.com/OME
<i>Dell EMC SupportAssist Enterprise User's Guide</i>	Provides information about installing, configuring, using, and troubleshooting SupportAssist Enterprise.	Dell.com/ServiceabilityTools
Troubleshooting Tool Online Help	Provides information about using the tool, related protocols, devices, and so on.	Integrated with the Troubleshooting Tool. From the Troubleshooting Tool, click the Help icon to launch the online help.
Dell EMC OpenManage Essentials MIB Import Utility Online Help	Provides information about the tool, importing and removing MIBs, troubleshooting procedures, and so on.	Integrated with the MIB Import Utility. From the MIB Import Utility, click the Help icon to launch the online help.

Contacting Dell

 **NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.**

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Go to **Dell.com/support**.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.

Installing OpenManage Essentials

Related links

- [Download OpenManage Essentials](#)
- [Installation prerequisites and minimum requirements](#)
- [Installing OpenManage Essentials](#)
- [Migrating IT Assistant to OpenManage Essentials](#)

Installation prerequisites and minimum requirements

For a list of supported platforms, operating systems, and browsers, see the *Dell EMC OpenManage Essentials Support Matrix* at Dell.com/OpenManageManuals.

To install OpenManage Essentials, you require local system administrator rights and the system you are using must meet the criteria mentioned in the **Minimum Requirements for OpenManage Essentials** section of the *Dell EMC OpenManage Essentials Support Matrix* available at Dell.com/OpenManageManuals.

Related link

- [Installing OpenManage Essentials](#)

Terms and conditions for using Relational Database Management Systems

The Relational Database Management System (RDBMS) used for installing OpenManage Essentials is Microsoft SQL Server. SQL Server has configuration settings separate from the OpenManage Essentials database. The server has logins (SQL or Windows) that may or may not have access to the OpenManage Essentials database.

When OpenManage Essentials is installed, Internet security is modified by adding registry entries to the ZoneMaps for HKLM and HKCU. This ensures that Internet Explorer identifies the fully qualified domain name as an intranet site.

A self-signed certificate is created and this certificate is installed in the root Certificate Authorities (CA) and My certificates.

To prevent certificate errors, remote clients must either install OpenManage Essentials certificate in both CA and Root Certificate Stores or have a custom certificate published to client systems by the domain administrator.

For a typical installation of OpenManage Essentials:

- Use the local instance of SQL Server that has all supported components.
- The RDBMS is altered to support both SQL and Windows authentication.
- An SQL Server login user is generated for OpenManage Essentials' services. This login is added as a RDBMS SQL login with the dbcreator role and given the db_owner role over the ITAssist and OMEssentials databases.



NOTE: The password for the typical install, auto generated SQL Server login account, is controlled by the application and different on every system.

For the highest level of security, it is recommended that you use a domain service account that is specified during custom installation for SQL Server.

At runtime, when the OpenManage Essentials website determines that it has an invalid certificate or certificate binding; the self-signed certificate is regenerated.


Related link

- [Minimum login roles for Microsoft SQL Server](#)

Minimum login roles for Microsoft SQL Server

The following table provides information about the minimum permissions for SQL Server based on different installation and upgrade use cases:

Table 2. Minimum login roles for Microsoft SQL Server

Number	Use Case	Minimum Login Roles for SQL Server
1	Installing OpenManage Essentials for the first time and you select the Typical option during the installation process.	sysadmin access on the installed instance.
2	Installing OpenManage Essentials for the first time, you select the Custom option during the installation process and an empty OpenManage Essentials database is present (locally or remotely).  NOTE: If you select the Custom install option and do not enter any credentials then the installation is considered as a Typical installation and sysadmin rights are required.	db_owner access on the OpenManage Essentials database.
3	You are installing OpenManage Essentials for the first time, you select the Custom option during the installation process, and an empty OpenManage Essentials database is not present.	dbcreator access on the server.
4	Upgrading OpenManage Essentials from an earlier version to the latest version and an OpenManage Essentials database is present (locally or remotely).	db_owner access on the OpenManage Essentials database.


Recommended database size

The following table provides information about the recommended database size for common use cases. However, it is recommended that you configure the database size based on the environment with different hardware configurations, and also regularly monitor the growth of the database size.

Table 3. Recommended database size

Recommended database size	Large deployments	Large deployments	Large deployments	Medium deployments	Small deployments
Number of devices	8000	5500	2000	500	100
SQL Server database size	14 GB	10 GB	6 GB	2 GB	1 GB

During the daily maintenance, OpenManage Essentials compresses and optimizes the database. Also, for optimal performance of OpenManage Essentials, monitor the database size and configure the Autogrowth/ Maxsize setting accordingly. It is recommended that the size of the log database must be 1.5 times the maximum size of the database. OpenManage Essentials also downloads updates for managed servers. These updates are saved in the local file system (not in the database) where OpenManage Essentials is installed.

 **NOTE:** OpenManage Essentials can maintain up to 175,000 task execution history details without any issues. If the task execution history details exceed 175,000, you may experience problems starting OpenManage Essentials. The earlier task execution history records are purged when the limit set under Task Settings → Task Execution History Records to be Retained is exceeded. The task execution history details of few tasks are not purged. For more information, see [Task Settings](#). It is recommended that you periodically delete task execution history details that you may no longer require or change the purge settings of task execution history details.

 **NOTE:** For more information, see the *OpenManage Essentials Scalability and Performance* technical white paper at DellTechCenter.com/OME.

Download OpenManage Essentials

Do keep the Service Tag of your Dell EMC PowerEdge server handy. It is recommended that you use the Service Tag to access all support on the Dell Support Website. This ensures that you download the appropriate version of the software for your platform.

To download OpenManage Essentials:

1. Go to Dell.com/support.
2. Perform one of the following actions:
 - Enter the Service Tag of your Dell EMC PowerEdge server, and then select Search.
 - Select **Browse all products** → **Servers** → **PowerEdge**, and select the appropriate model of your PowerEdge server.
3. On the support page of your server, select **Drivers & downloads**.
4. From the **Category** list, select **Systems Management**.
The supported version of OpenManage Essentials is displayed.
5. Click **Download** or select the check box to add the software to your download list.

Installing OpenManage Essentials

Before you install OpenManage Essentials, ensure that you have local administrator rights on the system.

 **NOTE:** OpenManage Essentials 2.5 use TLS version 1.2 to support Feature Usage Settings and the following features of MX7000 chassis—discovery, system update, device configuration template creation and deployment, and remediation. For more information about the best practices to be followed to secure .NET framework applications that use the TLS protocol on the management station, see www.docs.microsoft.com/en-us/dotnet/framework/network-programming/tls.

To install OpenManage Essentials:

1. Extract the OpenManage Essentials installation package.
2. Double-click the **Autorun.exe** file available in the folder where you extracted the installation package.
The **OpenManage Install** screen is displayed. The following options are available:
 - **Dell EMC OpenManage Essentials** — Select this option to install OpenManage Essentials, and Troubleshooting Tool.
 - **Dell EMC Repository Manager** — Select to install Repository Manager. Using Repository Manager, you can create customized bundles and repositories of Update Packages, software utilities such as update drivers, firmware, BIOS, and other applications.
 - **Dell EMC License Manager** — Select to install License Manager. The License Manager is a one-to-many license deployment and reporting tool for the integrated Dell Remote Access Controller (iDRAC), Chassis Management Controller (CMC), OpenManage Essentials, and the PowerEdge storage sled licenses.
 - **Dell EMC SupportAssist Enterprise** — Select to install SupportAssist Enterprise. The SupportAssist Enterprise provides proactive support capabilities for supported server, storage, and networking solutions.
 - **Documentation** — Click to view the online help.
 - **View Readme** — Click to view the readme file. To view the latest readme, go to DellTechCenter.com/OME.
3. In **OpenManage Install**, select **Dell EMC OpenManage Essentials**, and click **Install**.
The OpenManage Essentials Prerequisites window displays the following requirement types:
 - **Critical** — This error condition prevents the installation of a feature.


- **Warning** — This warning condition may disable the **Typical** installation but not an **Upgrade** of the feature later during installation. Also, later during installation, use the **Custom** installation setup type to select the feature.
- **Information** — This informational condition does not affect the **Typical** selection of a feature.

There are two options for resolving critical dependencies:


- Click **Install All Critical Prerequisites** to immediately begin installing all critical prerequisites without further interaction. **Install All Critical Prerequisites** may require a restart depending on the configuration and the prerequisites installation will resume automatically after restart.
- Install each prerequisite individually by clicking the associated link with the required software.

 **NOTE:** Ensure that KB2919355 update is installed on Windows 2012 R2 systems to run OpenManage Essentials 2.5. To install KB2919355 update manually, see the Microsoft Knowledge Base article ID 2919355 at support.microsoft.com.

 **NOTE:** The latest iDRAC and chassis firmware require TLS 1.1 and TLS 1.2 protocols to be enabled on Windows 2008 R2 and Windows 2012 systems. To enable TLS 1.1 and TLS 1.2 as the default secure protocols in WinHTTP, see the Microsoft Knowledge Base article ID 3140245 at support.microsoft.com.

 **NOTE:** To configure a remote database, you do not require an SQL Express installation on the local system. See [Setting Up OpenManage Essentials Database on a Remote SQL Server](#). If you are not configuring a remote database, then install SQL Express by clicking the warning prerequisite link. Selecting Install All Critical Prerequisites does not install SQL Express.

4. Click **Install Essentials**.


 **NOTE:** If you are installing OpenManage Essentials for the first time, a dialog box is displayed prompting you to select if you want to install OpenManage Essentials on a local or remote database. If you choose to install OpenManage Essentials on a local database, Microsoft SQL Server 2014 SP2 Express is installed on the system. If you choose to install OpenManage Essentials on a remote database, the installation follows the [Custom Setup Installation](#) steps.


5. In the install wizard for OpenManage Essentials, click **Next**.

6. In the **License Agreement** page, read the license agreement, select **I accept the terms in the license agreement**, and then click **Next**.

7. In **Setup type** select either **Typical** or **Custom** installation.

- If you selected **Typical**, click **Next**. Verify the installation settings in the **Ready to Install the Program** page and the click **Install**.

 **NOTE:** If the default ports assigned to the OpenManage Essentials services are either blocked or used by another application, a message is displayed prompting you to either unblock the ports or select the Custom installation where you can specify another port.

 **NOTE:** The parameters of all tasks that you create are encrypted and saved. During a reinstallation, if you choose to use a database that was retained from a previous OpenManage Essentials installation, the existing tasks will not run successfully. To resolve this issue, you must recreate all tasks after the installation.

- If you selected **Custom**, in **Custom Setup**, click **Next** and follow the instructions in [Custom Setup Installation](#).






8. After the installation is complete, click **Finish**.

If you have installed OpenManage Essentials on a virtual machine (VM), the following are the suggested settings for the OpenManage Essentials VM:

- Increase CPU settings based on resource availability.
- Disable **Dynamic Memory**.
- Increase **Memory Weight** to high.

Custom Setup Installation

To install OpenManage Essentials using custom setup:

1. In **Custom Setup**, click **Change** to change the installation location, and then click **Next**.
 2. In custom settings for port numbers, if required, change default values for **Network Monitoring Service port number**, **Task Manager Service port number**, **Package Server Port**, and **Console Launch port** and then click **Next**.
 3. In **Database Server**, do any of the following and then click **Next**:
 - Local database—If you have multiple SQL Server versions available on the management system and you want to select an SQL Server on which you want to set up the OpenManage Essentials database, then select the SQL server from the **Database Server** list, the type of authentication, and provide the authentication details. If you do not select a database server, by default, a supported version of SQL Server Standard, Enterprise, or Express that is available is selected for the installation. For more information, see the *Installing Dell OpenManage Essentials* technical white paper at DellTechCenter.com/OME.
 - Remote database— Complete the prerequisites. For more information, see [Setting Up OpenManage Essentials Database on a Remote SQL Server](#). After the prerequisites are complete, click **Browse** and select the remote system and then provide the authentication details. You can also set up the OpenManage Essentials database on a remote system by providing the IP address or host name and the database instance name of the remote system in **Database Server**.
-  **NOTE:** If you select the Custom install option and do not enter any credentials, the installation is considered as a typical installation and sysadmin rights are required.
-  **NOTE:** If you have multiple database instances running on a selected database server, you can specify the required database instance name to configure the Essentials database with it. For example, using (local)\MyInstance, you are configuring Essentials database on a local server and MyInstance named database instance.
-  **NOTE:** The parameters of all tasks that you create are encrypted and saved. During a reinstallation, if you choose to use a database that was retained from a previous OpenManage Essentials installation, the existing tasks will not run successfully. To resolve this issue, you must recreate all tasks after the installation.
-  **NOTE:** If you select the Custom install option, you can customize the database name. You can enter any name of your choice in the Database Name field. If you do not enter a database name, by default, OMEssentials is selected. Typically, you can use the database name field in a scenario where you have a dedicated remote SQL server that you want to use for installing multiple OpenManage Essentials instances. For example, you can assign the database name as DB_OME_Site1, DB_OME_Site2, and DB_OME_Site3 while installing the respective OpenManage Essentials instances.
-  **NOTE:** The database name must start with an alphabet and it should not exceed 80 characters in length. You may also include special characters in the database name, except square brackets ([]), apostrophe ('), and curly brackets ({}).
4. Verify the installation settings in the **Ready to Install the Program** page and the click **Install**.

Setting up OpenManage Essentials Database on a Remote SQL Server

You can configure OpenManage Essentials to use an SQL Server present on a remote system. Before setting up the OpenManage Essentials database on the remote system, check for the following prerequisites:

- Network communication between the OpenManage Essentials system and the remote system is functioning.
- SQL connection works between the OpenManage Essentials system and the remote system for the specific database instance. You can use the **Microsoft SQL Server Express 2012 Management Studio** tool to verify the connection. On the remote database server, enable TCP/IP protocol and if you are using SQL Authentication, enable mixed mode on the remote SQL Server.

You can retarget the database if:

- SQL credential to the SQL Server fails.
- Windows credential to the SQL Server fails.
- Login credentials have expired.

- Database is moved.

Retargeting the OpenManage Essentials Database

You can setup the OpenManage Essentials console to connect to an OpenManage Essentials database available on a remote system. For example, after installing OpenManage Essentials with a local database, you can back up and restore the OpenManage Essentials database on a remote system. After the database is restored on the remote system, you can setup OpenManage Essentials to connect to the restored database available on the remote system.

To retarget the OpenManage Essentials database:

1. Back up the OpenManage Essentials database. See [Backing up the OpenManage Essentials Database](#).
2. Restore the OpenManage Essentials database. See [Restoring the OpenManage Essentials Database](#).
3. Create a new user in SQL Server. See [Creating a new user in SQL Server](#).
4. Connect to the OpenManage Essentials database. See [Connecting to the OpenManage Essentials Database](#).

Backing up the OpenManage Essentials Database

Before you back up the OpenManage Essentials database:

- Ensure that OpenManage Essentials is installed on the system using the **Typical** installation method.
- Ensure that Microsoft SQL Server Management Studio is installed on the system where OpenManage Essentials is installed.
- Ensure that you stop Internet Information Services (IIS) and all OpenManage Essentials services.

To back up the OpenManage Essentials database:

1. Open SQL Server Management Studio.
2. In **Object Explorer**, expand the **Databases** node.
3. Right-click the **OMEssentials** database and then click **Tasks** → **Back Up**.
The **Back Up Database - OMEssentials** window is displayed.
4. Click **OK** to start the database back up.

A confirmation message is displayed after the database back up is completed. The OpenManage Essentials database backup file, **OMEssentials.bak**, is saved at **C:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\OME\MSSQL\Backup**.

Restoring the OpenManage Essentials Database


Before you begin to restore the OpenManage Essentials database:

- Ensure that OpenManage Essentials database back up file, **OMEssentials.bak**, is available on the system. If required, you must copy and paste the OpenManage Essentials database back up file from the system where you created the back up file.
- Ensure that Microsoft SQL Server Management Studio is installed on the system.
- Ensure that you have sysadmin access for SQL Server.

To restore the OpenManage Essentials database:

1. Open SQL Server Management Studio on the system where you want to restore the OpenManage Essentials database.
2. In **Object Explorer**, right-click **Databases** → **Restore Database**.
The **Restore Database** window is displayed
3. Under **Source**, select **Device** and click the browse button.
The **Select backup devices** window is displayed.
4. Click **Add** and then browse to select the OpenManage Essentials database back up file.
5. Click **OK** to close the **Select backup devices** window.
6. Click **OK** in the **Restore Database** window to start restoring the database.

A confirmation message is displayed after the database is restored. The restored **OMEssentials** database is displayed under **Databases** in **Object Explorer**.

 **NOTE:** The database restoration may not be successful if multiple instances of the backup file, OMEssentials.bak, are available on the system. To resolve the issue, rename both the files (OMEssentials and OMEssentials_log) in the Restore database file as section of the Restore Database window, and then try restoring the database.

Creating a new user in SQL Server

To create a new user in SQL Server:

1. Open SQL Server Management Studio on the system where you restored the OpenManage Essentials database.
2. In **Object Explorer** expand the **Security** node.
3. Click **Login** → **New Login**.
The **Login - New** window is displayed.
4. In the **General** page:
 - a. Type a name in the **Login name** field.
 - b. Select **Windows authentication** or **SQL Server authentication** based on your preference.
 - c. Type the password and reconfirm the password in the appropriate fields.
 - d. Optional: If you want to enforce password policy options for complexity, select **Enforce Policy Password**.
 - e. From the **Default database** list, select **OMEssentials**.
 - f. From the **Default language** list, select a default language for the login.
5. In the **Server Roles** page, select **public**.
6. In the **User Mappings** page:
 - a. Under **Users mapped to this login**, select **OMEssentials**.
 - b. Under **Database role membership for: OMEssentials**, select **db_owner** and **public**.
7. Click **OK**.

The new user that you created is displayed under **Security** → **Logins** in **Object Explorer**.

Connecting to the OpenManage Essentials Database

To connect to the OpenManage Essentials database:

1. On the system where OpenManage Essentials is installed, open the command prompt, and run the following command:
`sqlcmd -E -S ".\SQLEXPRESSOME" -Q "ALTER LOGIN [OMEService] WITH PASSWORD='DummyPassword'"`

 **NOTE:** Verify that the OpenManage Essentials database instance that was created during the typical installation is SQLEXPRESSOME.


 **NOTE:** Copying and pasting the command may result in incorrect characters. Therefore, it is recommended that you type the complete command.

2. Open OpenManage Essentials.
The database login error window is displayed.
3. Click **OK** on the database login error window.
The **Database Connection Error** window is displayed.
4. In the **Database Connection Error** window:
 - a. In the **Server Name** field, type the name of the system where you restored the OpenManage Essentials database.
 - b. From the **Authentication** list, select the authentication method for the database.
 - c. Type the user name and password of the new user you created in the appropriate fields.
 - d. Type the name of the database that you have already created in SQL Server.
 - e. Click **Connect**.
5. Close and reopen OpenManage Essentials.
6. Restart the Internet Information Services (IIS).
7. Restart the OpenManage Essentials services or restart the server.

After the database retargeting is completed successfully, if required, you can delete the OpenManage Essentials database from the system on which OpenManage Essentials is installed.

Installing OpenManage Essentials on a domain controller

When installing OpenManage Essentials on a domain controller, it is recommended that you install OpenManage Essentials with a remote database. There are specific restrictions when running SQL Server on a domain controller, and considering the resources demands of a domain controller, SQL Server performance may be degraded which will affect the performance of OpenManage Essentials. For more information on the restrictions when running SQL Server on a domain controller, see the Microsoft Knowledge Base article ID 2032911 at support.microsoft.com.

 **NOTE: For security reasons, it is recommended that you do not install SQL Server 2012 on a domain controller. SQL Server Setup will not prevent you from installing SQL Server on a domain controller, however, the following limitations apply:**

- You cannot run SQL Server services on a domain controller under a local service account.
- After SQL Server is installed on a system, you cannot change the system from a domain member to a domain controller. You must uninstall SQL Server before you change the host system to a domain controller
- SQL Server failover cluster instances are not supported where cluster nodes are domain controllers.
- SQL Server Setup cannot create security groups or provision SQL Server service accounts on a read-only domain controller. In this scenario, Setup will fail.

When setting up OpenManage Essentials on a domain controller, ensure that the following prerequisites are met:

- Ensure that network communication between the system on which OpenManage Essentials is installed and the remote database system is functional.
- Ensure that the SQL Server user has permission to backup, create, and configure databases.
- When using SQL Server authentication, ensure that SQL Server and Windows authentication mode is enabled within SQL Server. See [Enabling SQL Server Authentication and Windows Authentication in SQL Server](#)
- Ensure that TCP/IP is enabled in SQL Server. See [Verifying the SQL Server TCP/IP status](#).

After OpenManage Essentials is installed on a domain controller:

- By default, the **Domain Admins** group is added as a member of the **OmeAdministrators** and **OmePowerUsers** roles.
- Local Windows user groups are not included in the OpenManage Essentials roles. **OmeAdministrators**, **OmePowerUsers**, or **OmeUsers** rights can be granted to users or user groups by adding them to the OpenManage Essentials Windows groups. **OmeSiteAdministrators** rights can be granted by **OmeAdministrators** through the **Device Group Permissions** portal.


The following sections provide instructions to install and setup OpenManage Essentials on a domain controller with a remote or local database.

Installing OpenManage Essentials on a domain controller with a remote database


Before you begin installing OpenManage Essentials on a domain controller, ensure that you are logged in to the domain controller with administrator rights.

To install OpenManage Essentials on a domain controller with a remote database:

1. Extract the OpenManage Essentials installation package.
2. Double-click the **Autorun.exe** file available within the folder where you extracted the installation package.
The **OpenManage Install** window is displayed.
3. Select **Dell EMC OpenManage Essentials** and click **Install**.
The OpenManage Essentials Prerequisites window is displayed.
4. Click **Install All Critical Prerequisites**.


 **NOTE:** If SQL Server is not already installed on the domain controller, the Prerequisites window displays a warning message with a link that allows you to install SQL Express on the domain controller (local) with an OpenManage Essentials-specific SQLEXPRESSOME database instance. If you ignore the warning message, when the OpenManage Essentials installation begins, a message is displayed requesting you to confirm whether you want to install OpenManage Essentials with a local or remote database

5. When the confirm database location message is displayed, click **No** to install OpenManage Essentials on a remote database. The **Custom Setup** window is displayed.
6. Click **Next**.
The **OpenManage Essentials Custom Settings** window is displayed.
7. If required, change the default port numbers based on your requirement, and click **Next**.
The **Database Server** window is displayed.
8. Perform one of the following:
 - Click **Browse** and select the remote database.
 - Type the host name and database instance name in the **Database Server** field.
9. Click **Windows authentication** or **SQL Server authentication**.

 **NOTE:** For Windows authentication, if you are using a non-domain Windows account, the credentials must exist on both the domain controller and the remote system, and should also be identical. The Windows user account must have the privileges required to create databases in SQL Server.

10. Type the user name and password in the appropriate fields and click **Next**.
The **Ready to Install the Program** window is displayed.
11. Click **Install**.

After the installation of OpenManage Essentials is completed, add the logged in administrator to the OMEAdministrators user group. See [Adding Users to the OpenManage Essentials Groups](#).


 **NOTE:** After the OpenManage Essentials database is set up on the remote system, if the database is either moved or altered, open OpenManage Essentials to re-target using the new database connection settings.

Installing OpenManage Essentials on a domain controller with a local database

Before you begin installing OpenManage Essentials on a domain controller, ensure that you are logged in to the domain controller with administrator rights.

To install OpenManage Essentials on a domain controller with a local database:

1. Extract the OpenManage Essentials installation package.
2. Double-click the **Autorun.exe** file available within the folder where you extracted the installation package.
The **OpenManage Install** window is displayed.
3. Select **Dell EMC OpenManage Essentials** and click **Install**.
The OpenManage Essentials Prerequisites window is displayed.

 **NOTE:** If SQL Server is not already installed on the domain controller, the Prerequisites window displays a warning message with a link that allows you to install SQL Express on the domain controller (local) with an OpenManage Essentials-specific SQLEXPRESSOME database instance.

4. In the **Prerequisites** window, click the link to install SQL Express on the domain controller.
5. Create a domain service account required to run SQL Server on the domain controller. See [Creating a Domain Service Account](#).
6. Configure the SQLEXPRESSOME instance to run using the domain service account. See [Configuring the Database Instance](#).
7. Click **Install Essentials** on the **Prerequisites** window, and follow the instructions on the screen to complete the installation of OpenManage Essentials.

After the installation of OpenManage Essentials is completed, add the logged in administrator to the OMEAdministrators user group. See [Adding Users to the OpenManage Essentials User Groups](#).

Creating a Domain Service Account

A domain service account is required to run SQL Server on the domain controller.

To create a domain service account:

1. Click **Start** → **Administrative Tools**.
2. Select **Active Directory Users and Computers**.
3. On the left pane, right-click **Managed Service Account** → **New** → **User**.
The **New Object – User** window is displayed.
4. Type the first name and user logon name in the appropriate fields, and click **Next**.
5. Type a password and reconfirm the password in the appropriate fields, and click **Finish**.

Configuring the database instance


The SQL Server service will not start if you are using the default NETWORK SERVICE or LOCAL SYSTEM accounts. Therefore, you must configure the SQLEXPRESS database instance to run using a domain service account.

To configure the SQLEXPRESS database instance:

1. Open Microsoft SQL Server Configuration Manager.
2. On the left pane, click **SQL Server Services**.
3. On the right-pane, right-click **SQL Server (SQLEXPRESS)** and click **Properties**.
The **SQL Server (SQLEXPRESS) Properties** window is displayed.
4. In the **Log on** tab, select **This account**.
5. Type the domain service account name, password, and confirm the password in the appropriate fields.
6. Click **Restart**.
7. Click **Apply**.

Adding users to the OpenManage Essentials user groups

To add users to the OpenManage Essentials user groups:

 **NOTE:** The users you add to the OpenManage Essentials user group must also belong to the built-in local Administrator group. For information on adding a Windows user account to a group, see *Adding a user account to a group* at support.microsoft.com

1. Open Server Manager.
2. Click **Tools** → **Computer Management**.
3. In the left pane, click **Local Users and Groups** → **Groups**.
4. In the right-pane, right-click **OmeAdministrators** and select **Add to Group**.
5. In the **OmeAdministrator Properties** window, click **Add**.
The **Select Users** window is displayed.
6. In the **Enter the object names to select** field, type the user name.
7. Click **Check Names** and then click **OK**.
The user name is displayed in the **Members** list within the **OmeAdministrator Properties** window.
8. Click **OK**.

Enabling SQL Server and Windows Authentication Mode in SQL Server

To enable SQL Server and Windows authentication mode:

1. Open SQL Server Management Studio.
2. In **Object Explorer**, right-click the top-level SQL Server object and click **Properties**.
The **Server Properties** window is displayed.
3. In the left pane, click **Security**.
4. In the right pane, under **Server authentication**, click **SQL Server and Windows Authentication mode**.

5. Click **OK**.
6. In **Object Explorer**, right-click the top-level SQL Server object and click **Restart**.

Verifying SQL Server TCP or IP Status

To verify the TCP/IP status of SQL Server:

1. Click **Start** → **All Programs** → **SQL Server Configuration Manager**



NOTE: If multiple versions of SQL Server Configuration Manager are installed, ensure that you select the latest version.

2. On the left pane, click to expand **SQL Native Client 11.0 Configuration**.
3. Click **Client Protocols**.
4. On the right pane, ensure that the status of TCP/IP is **Enabled**.
5. If TCP/IP is not enabled, right-click TCP/IP and select **Enable**.

Installing SupportAssist Enterprise

SupportAssist Enterprise integrates with OpenManage Essentials to provide proactive support capabilities for enterprise servers, storage, and networking solutions using the existing environment data. SupportAssist collects information from supported devices, and automatically creates support cases when issues arise. This helps Dell EMC to provide you an enhanced, personalized, and efficient support experience.

To install SupportAssist:



NOTE: Before you begin, make sure that:

- The system is able to connect to the Internet.
- You have the Administrator rights on the system.
- On the firewall, port 443 is open to access <https://ftp.dell.com>.

1. Extract the OpenManage Essentials installation package.
2. In the folder where you extracted the installation package, double-click the **Autorun.exe** file.
The **OpenManage Install** window is displayed.
3. If OpenManage Essentials version 2.5 is not installed on the system, make sure that **Dell EMC OpenManage Essentials** is selected.
4. Select **Dell EMC SupportAssist Enterprise**, and then click **Install**.

If you selected **Dell EMC OpenManage Essentials** and **Dell EMC SupportAssist Enterprise**, installation of OpenManage Essentials is completed and then SupportAssist Enterprise is installed. The system prerequisites for installing SupportAssist Enterprise are verified. If the system prerequisites are met, the **Welcome to Dell EMC SupportAssist Enterprise Installer** window is displayed.

5. Click **Next**.
The **License Agreement** window is displayed.
6. Read the terms in the communication requirements and click **I Agree**.



NOTE: SupportAssist Enterprise installation requires that you allow Dell EMC to save certain Personally Identifiable Information (PII) such as your contact information, administrator credentials of the devices to be monitored, and so on. SupportAssist installation cannot proceed unless you allow Dell EMC to save your PII.

7. Read the software license agreement, click **I Agree**, and then click **Next**.
If the system connects to the Internet through a proxy server, the **Proxy Settings** window is displayed. Else, the **Installing SupportAssist Enterprise** window is displayed briefly, and then the **Installation Completed** window is displayed.
8. If the **Proxy Settings** window is displayed, provide the following:
 - a. In the **Server Address** field, type the proxy server address or name.
 - b. In the **Port** field, type the proxy port number.



NOTE: If the proxy server credentials are not provided, SupportAssist Enterprise connects to the proxy server as an anonymous user.

- c. If the proxy server requires authentication, select **Proxy requires authentication**, and then provide the following information in the corresponding fields:
 - **Username** — The user name must contain one or more printable characters, and must not exceed 104 characters.
 - **Password** — The password must contain one or more printable characters, and must not exceed 127 characters.
 - **Confirm Password** — Re-enter the password. The password must match with the one provided in the **Password** field.
 - d. Click **Install**.
The proxy settings are validated. If the validation is unsuccessful, verify the proxy settings and try again or contact your network administrator for assistance.
 - e. In the **Validation Successful** dialog box, click **OK**.
The **Installing SupportAssist Enterprise** window is displayed briefly, and then the **Installation Completed** window is displayed.
9. Click **Finish**.

When you start SupportAssist Enterprise, the **SupportAssist Enterprise Setup Wizard** is displayed. You must complete all steps in the **SupportAssist Enterprise Setup Wizard** before you can use SupportAssist Enterprise. For more information, see the *Dell EMC SupportAssist Enterprise User's Guide* at www.dell.com/ServiceabilityTools.



NOTE: If the installation of SupportAssist Enterprise fails, you can retry the installation later. To retry the installation, right-click the Dell EMC SupportAssistSetup.exe file available at C:\Program Files\Dell\SysMgt\Essentials \SupportAssistSetup and select Run as administrator.

Installing Repository Manager

The Repository Manager is an application that helps manage system updates easily and effectively. Using Repository Manager, you can build a custom repository based on the managed system configurations that are obtained from OpenManage Essentials.

To install Repository Manager:

1. Double-click the OpenManage Essentials executable file.
2. In **OpenManage Install**, select **Dell EMC Repository Manager**, and then click **Install**.
3. In **Dell EMC Repository Manager - InstallShield Wizard**, click **Next**.
4. In **License Agreement**, select **I accept the terms in the license agreement**, and click **Next**.
5. In **Customer Information**, do the following and click **Next**.
 - a. Provide user name and organization information.
 - b. Select either **Anyone who uses this computer (all users)** to make this application available to everyone or **Only for me (Windows User)** to retain access.
6. In **Destination Folder**, use the default location or click **Change** to specify another location, and then click **Next**.
7. In **Ready to Install the Program**, click **Install**.
8. After the installation is complete, click **Finish**.

Installing License Manager

The License Manager is a one-to-many license deployment and reporting tool for the integrated Dell Remote Access Controller (iDRAC), Chassis Management Controller (CMC), OpenManage Essentials, and the PowerEdge storage sled licenses.

To install License Manager:

1. Double-click the OpenManage Essentials executable file.
2. In **OpenManage Install**, select **Dell EMC License Manager**.
3. Select a language for the installation, and click **OK**.
4. In the **Welcome** screen, click **Next**.
5. In **License Agreement**, select **I accept the terms in the license agreement** and click **Next**.
6. In **Setup Type**, select any of the following:

- To accept the default installation path, choose **Typical** installation and click **Next**.
 - To enable specific program features and change the installation path, select **Custom** installation and click **Next**. In **Custom Setup**, select the License Manager features that you require; check for disk space, assign a new location for installing License Manager.
7. In the **Ready to Install** screen, click **Install**.
 8. After the installation is complete, click **Finish**.


Upgrading OpenManage Essentials

You can upgrade from OpenManage Essentials version 2.1 and later to OpenManage Essentials version 2.5. Before you upgrade, ensure that the minimum available free space on the hard drive is about 10 GB.


 **NOTE: OpenManage Essentials 2.5 use TLS version 1.2 to support Feature Usage Settings and the following features of MX7000 chassis—discovery, system update, device configuration template creation and deployment, and remediation. For more information about the best practices to be followed to secure .NET framework applications that use the TLS protocol on the management station, see www.docs.microsoft.com/en-us/dotnet/framework/network-programming/tls.**

To upgrade:

1. Double-click the OpenManage Essentials executable file.
The **Dell OpenManage Install** screen is displayed. The following options are available:
 - **Dell EMC OpenManage Essentials** — Select this option to install OpenManage Essentials, and Troubleshooting Tool.
 - **Dell EMC Repository Manager** — Select this option to install Repository Manager. Using Repository Manager, you can create customized bundles and repositories of Update Packages, software utilities such as update drivers, firmware, BIOS, and other applications.
 - **Dell EMC License Manager** — Select this option to install License Manager. The License Manager is a one-to-many license deployment and reporting tool for the integrated Dell Remote Access Controller (iDRAC), Chassis Management Controller (CMC), OpenManage Essentials, and PowerEdge storage sled licenses.
 - **Dell EMC SupportAssist Enterprise** — Select this option to install SupportAssist Enterprise. The SupportAssist Enterprise provides proactive support capabilities for supported server, storage, and networking solutions.

 **NOTE: If SupportAssist Enterprise is already installed on the system, by default, the Dell EMC SupportAssist Enterprise option is selected and disabled. After the upgrade of OpenManage Essentials, SupportAssist Enterprise is also upgraded. If applicable, you may be required to provide the proxy settings during the upgrade of SupportAssist Enterprise. For more information, see the *Dell EMC SupportAssist User's Guide* at www.dell.com/ServiceabilityTools.**

 - **Documentation** — Click to view the online help.
 - **View Readme** — Click to view the readme file. To view the latest readme, go to DellTechCenter.com/OME.
2. In the **OpenManage Install** screen, select **Dell EMC OpenManage Essentials** and click **Install**.
The **OpenManage Essentials Prerequisites** window, displays the following requirement types:
 - **Critical** — This error condition prevents the installation of a feature.
 - **Warning** — This warning condition may disable the **Typical** installation but not an **Upgrade** of the feature later during installation.
 - **Information** — This informational condition does not affect the **Typical** installation of a feature.

 **NOTE: If OpenManage Essentials version 1.1 is installed on the system on a local database using SQL Server 2008 Express edition, and an OpenManage Essentials-specific named instance SQLEXPRESSOME is not available, the SQL Server prerequisites displays a Critical icon. To proceed with the installation, you must install SQL Server Express 2012 SP1 with the SQLEXPRESSOME instance. Data from the earlier version of SQL Server is migrated automatically.**
3. Click **Install Essentials**.
4. In the install wizard for OpenManage Essentials, click **Next**.
5. In the **License Agreement** page, read the license agreement, select **I accept the terms in the license agreement**, and then click **Next**.
6. If applicable, provide the **Package Server Port** and the **Task Manager Service Port**. If either the package server port or task manager service port is blocked during an upgrade, provide a new port. Click **Next**.

 **NOTE:** For information about the supported ports and protocols, see [Supported protocols and ports in OpenManage Essentials](#).

7. Click **Ok**.
8. Click **Install**.
9. After the installation is complete, click **Finish**.

After the upgrade, when you launch OpenManage Essentials version 2.5 for the first time, the **Feature Usage Settings** window is displayed. To understand and improve the most used features in OpenManage Essentials, few nonsensitive information is collected, and this feature is enabled by default. To disable this feature at a later time, click **Settings → Feature Usage Settings**, and then clear the **I Agree** check box.

After the upgrade is complete, you must perform the following actions:

1. Run discovery and inventory for all existing discovery ranges.
2. In the **Device Search** portal, verify if you get the expected results for all existing device queries.
3. In the **System Update** portal, if the existing catalog is not the latest, ensure you import the latest catalogs from downloads.dell.com.

Reconfiguring OpenManage Essentials version 2.5 after upgrading

This section contains information about the changes in templates on the Deployment portal, baselines in the Configuration portal, and tasks that must be performed after upgrading to OpenManage Essentials version 2.5 from OpenManage Essentials version 2.2 and earlier.

The upgraded version of OpenManage Essentials provide the following enhancements:

- Enhanced configuration settings for the Chassis templates and baselines with user-friendly attribute names.
- Enhanced details about changed attributes for Chassis Deployment.
- Create baselines for server and chassis from corresponding server or chassis templates that were available in the earlier version of OpenManage Essentials. The newly created server and chassis baseline names are suffixed with **Baseline**.

 **NOTE:** Baselines are used for device compliance.

- Provides the option to recreate the Chassis template for deployment and the Chassis baseline for compliance-related tasks.

 **NOTE:** After upgrading to OpenManage Essentials 2.5, the template deployment tasks are available under **Deployment → Tasks**.

- Provides the option to discover devices based on specific device type and specific protocol. For more information, see [Configuring the Discovery Wizard](#).

After the upgrade is complete, you must perform the following tasks:

- From the **Deployment** portal, recreate the Chassis Template. For more information, see [Recreating chassis template](#).
- From the **Manage → Configuration portal**, recreate the Chassis Baseline. For more information see [Recreating chassis baseline](#).
- Recreate the scheduled chassis deployment tasks that were created in OpenManage Essentials version 2.2 and earlier as the scheduled chassis deployment task cannot be edited or rerun after upgrading to OpenManage Essentials version 2.5. The user can edit the scheduled task that is created after the upgrade.

 **NOTE:** Ensure that the recreated chassis template and baseline are reviewed, and required changes and selection are made to the attribute values.

Recreating chassis template

After upgrading to the latest version of OpenManage Essentials, the existing chassis templates, which were created in OpenManage Essentials version 2.2 and earlier, are displayed as broken.

To recreate the chassis template:

1. Click **Deployment → Templates**.
2. From the **Chassis Templates**, select a template.
3. On the **Template action** window, click the **Recreate this Template** button to recreate the chassis template.
4. On the **Task Authentication** window, type the template credentials and click **OK**.

A 'Create template' task is submitted for execution.

5. Click **OK**.

The selected chassis template is recreated.

 **NOTE: The recreated chassis template name is not changed.**

6. Click the recreated chassis template and click the **Attributes** tab to make the desired changes to the template attributes.

 **NOTE: For compliance and deployment related tasks, ensure that the chassis has an enterprise license, supported firmware version, and is discovered by using the WS-Man protocol. For more information, see [Device requirements for deployment and compliance tasks](#).**

 **NOTE: The chassis template which is created from a file does not display the Recreate this Template button and has to be recreated manually from the chassis configuration file.**

Recreating chassis baseline

OpenManage Essentials 2.5 automatically creates a corresponding chassis baseline for the chassis template that was created in OpenManage Essentials version 2.2 and earlier after upgrading. The chassis baseline that is created after the upgrade has the baseline name suffixed with **Baseline**. The chassis baselines are displayed as broken in the **Configuration** portal and must be recreated.

To recreate the chassis baseline:

1. Click **Manage** → **Configuration** → **Compliance by Baseline** → **Chassis Baseline**.
2. From **Chassis Baselines**, select a baseline.
3. On the **Baseline action** window, click the **Recreate this Baseline** button to recreate the chassis baseline.
4. On the **Task Authentication** window, type the chassis credentials and click **OK**.

A 'Create baseline' task is submitted for execution.

5. Click **OK**.

The selected chassis baseline is recreated.

 **NOTE: The recreated baseline name is not changed.**

 **NOTE: While recreating the chassis baseline, OpenManage Essentials will automatically take care of all the devices that are associated with the baseline in the earlier version and the compliance-related tasks.**

6. Click the recreated baseline and click the **Attributes** tab to check the baseline attributes.

 **NOTE: For compliance and deployment related tasks, ensure that the chassis has an enterprise license, supported firmware version, and is discovered by using the WS-Man protocol. For more information, see [Device requirements for deployment and compliance tasks](#).**

 **NOTE: The chassis baseline which is created from a file does not display the Recreate this Template button and has to be recreated manually from the chassis configuration file.**

Uninstalling OpenManage Essentials

 **NOTE: Before uninstalling OpenManage Essentials, you must uninstall OpenManage Essentials MIB Import Utility and SupportAssist Enterprise (if installed).**

To uninstall OpenManage Essentials:

1. Click **Start** → **Control Panel** → **Programs and Features**.
2. In **Uninstall or change a program**, select **Dell EMC OpenManage Essentials** and click **Uninstall**.
3. In the message **Are you sure you want to uninstall OpenManage Essentials?**, click **Yes**.
4. In the message **Uninstalling OpenManage Essentials removes the OpenManage Essentials database. Do you want to retain the database?**, click **Yes** to retain the database or click **No** to remove it.
5. Click **Finish**.

Migrating IT Assistant to OpenManage Essentials

Direct migration from IT Assistant to OpenManage Essentials version 2.5 is not supported. However, you can migrate IT Assistant to an earlier version of OpenManage Essentials, and then upgrade to OpenManage Essentials version 2.5. For information about migrating IT Assistant to an earlier version of OpenManage Essentials, see the appropriate *Dell EMC OpenManage Essentials User's Guide* at Dell.com/OpenManageManuals.

Related link

[Installing OpenManage Essentials](#)

Getting started with OpenManage Essentials

Launching OpenManage Essentials

To launch OpenManage Essentials, do one of the following:

 **NOTE:** Before you launch OpenManage Essentials, ensure that Javascript is enabled on your web browser.

- From the management station desktop, click the **Essentials** icon.
- From the management station desktop, click **Start** → **All Programs** → **Dell EMC OpenManage Applications** → **Essentials** → **Essentials**.
- From a local or remote system, launch a supported browser. In the address field, type any of the following:
 - **https://< Fully Qualified Domain Name (FQDN) >:**
 - **https://<IP address, host name, or Fully Qualified Domain Name (FQDN) >:<Port Number>/web/default.aspx**
 - **https://<IP address>:<Port Number>/**

 **NOTE:** FQDN is required to show a valid certificate. The certificate shows an error if an IP address or local host is used.

The console launch port number (default port number 2607) is required to launch OpenManage Essentials from a browser on a remote system. While installing OpenManage Essentials, if you changed the port using the **Custom Install** option, use the selected console launch port in the preceding URL.

When you launch OpenManage Essentials version 2.5 for the first time, the **Feature Usage Settings** window is displayed. To understand and improve the most used features in OpenManage Essentials, few nonsensitive information is collected, and this feature is enabled by default. To disable this feature at a later time, click **Settings** → **Feature Usage Settings**, and then clear the **I Agree** check box.

Next, the **First Time Setup** page is displayed.

 **NOTE:** You can log in to OpenManage Essentials as a different user at any time by using the **Sign in as Different User** option. For more information, see [Logging On As a Different User](#).

Related link

[Using the OpenManage Essentials Home Portal](#)

Configuring OpenManage Essentials

If you are logging on to OpenManage Essentials for the first time, the **First Time Setup** tutorial is displayed. The tutorial provides step-by-step instructions for setting up an environment of servers and devices to communicate with OpenManage Essentials. The steps include:

- Configuring the SNMP protocol on each target server.
- Installing SNMP tools (for Windows Server 2012 or later).
- Installing OpenManage Server Administrator on each target server.
- Enabling network discovery (for Windows Server 2008-based servers) on each target server.
- Discovering devices on your network.

After you have completed the **First Time Setup** wizard, the **Discovery Wizard Configuration** window is displayed. See [Discovery Wizard Configuration](#).

The date and time displayed in the console is in a format that is selected in the browser settings and used in the region. When a time zone change or daylight savings change occurs, the time is updated accordingly in the console. Changing time zones or daylight savings, changes the time in the console, but does not change the time in the database.



Related link

[Using the OpenManage Essentials Home Portal](#)

Configuring the Discovery Wizard

The **Discovery Wizard Configuration** window enables you to configure the type of wizard you want to use for discovering devices. The options displayed in the **Discovery Wizard Configuration** window are described in the following table.

Table 4. Discovery Wizard Configuration

Option	Description
Standard Wizard	If selected, the Discover Devices wizard displays a list of protocols for discovering devices.
Guided Wizard (default)	If selected, the Discover Devices wizard displays a list of device types and the required protocols for discovering and managing the selected devices. After the required protocol configurations are completed, by default, this wizard runs both discovery and inventory.  NOTE: Discovery of storage arrays is not supported by the Guided Wizard.
Skip ICMP ping during discovery	If selected, the ICMP Configuration settings will be disabled from the Discover Devices wizard. By selecting this option, ICMP ping is skipped during discovery and inventory of the devices, system updates, configuration and deployment tasks.
Discover the selected Device Types only	In OpenManage Essentials 2.5, this option is enabled by default. If selected, this option allows device-type discovery in the guided wizard.  NOTE: The device range that was discovered in the earlier version of OME may have discovered both chassis and iDRAC using WS-MAN protocol. In OpenManage Essentials 2.5, if Discover the selected Device Types only option is enabled in Discovery settings, then only the specific device selected in the guided wizard will be discovered and other devices are classified as unknown devices. For example: Selecting iDRAC device type with WS-MAN protocol will discover only iDRAC devices using WS-MAN protocol.

After you select the type of wizard and click **Finish**, the setting is saved in **Settings** → **Discovery Settings**.

By default, the **Discovery Wizard Configuration** window is displayed when you:

- Launch OpenManage Essentials for the first time.
- Click **Add Discovery Range** in the **Discovery and Inventory** portal for the first time.

If you want to configure the type of wizard you want to use for discovering devices at a later time, you can do so through the **Discovery Settings** page. For more information, see [Configuring Discovery Settings](#).

Configuring Discovery Settings

The **Discovery Settings** page enables you to configure the type of wizard you want to use for discovering devices.

To configure discovery settings:

1. Click **Settings** → **Discovery Settings**.

The **Discovery Settings** page is displayed.

2. Select one of the following:

- **Standard Wizard** — If selected, the **Device Discovery** wizard displays a list of protocols for discovering devices.
- **Guided Wizard** — If selected, the **Device Discovery** wizard displays a list of device types and the required protocols for discovering and managing the selected devices. After the required protocol configurations are completed, by default, this wizard runs both discovery and inventory.

 **NOTE: Discovery of storage arrays is not supported by the Guided Wizard.**

3. Click **Apply**.

Using the OpenManage Essentials Home Portal

OpenManage Essentials user interface contains the following components:

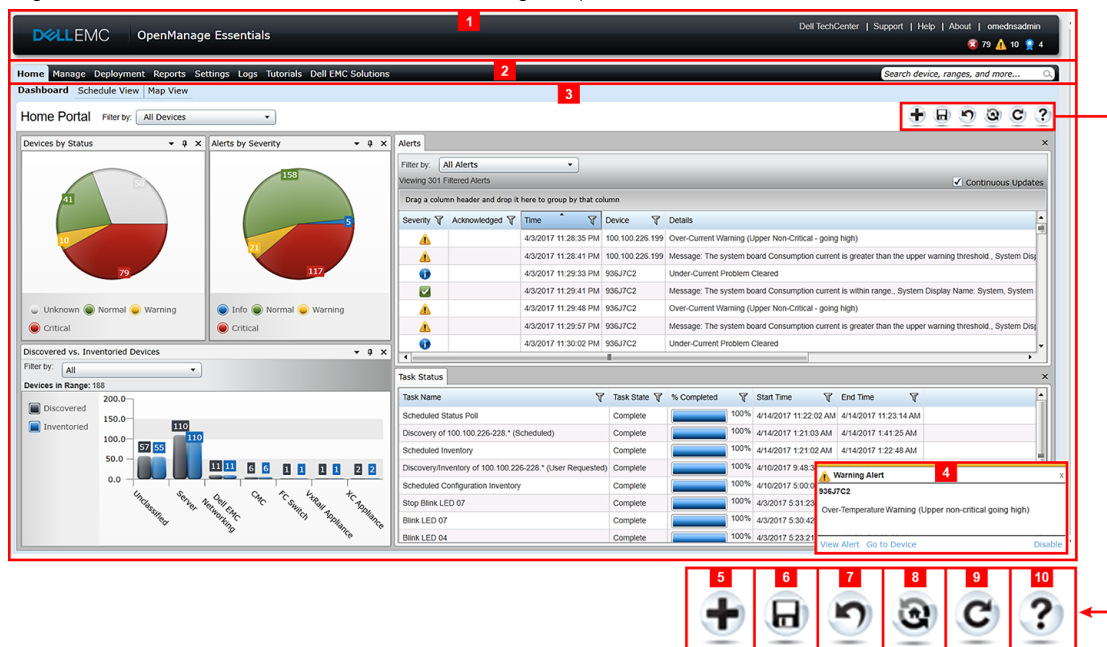


Figure 1. OpenManage Essentials Home Portal

1. Heading banner
2. Menu items and search bar
3. Console area
4. Alert pop-up notification
5. Add a report to the home portal
6. Save the current home portal layout
7. Load the last saved home portal layout
8. Load the default home portal layout
9. Refresh the home portal page
10. Launch the online help

Related links






[Map View—Home Portal](#)

[Dashboard](#)

[Using the Search Bar](#)

OpenManage Essentials Heading Banner

The banner may display the following icons:

- Critical icon  and Warning icon  including the number of devices. You can click the icon or the number to view the devices in either state.
- OpenManage Essentials service not running icon (blinking down arrow) . You can click the icon to view the details and to restart the service.
- Update available notification icon  indicates if a newer version of OpenManage Essentials is available. Click the icon to open a **New Version Available** window that displays the currently installed and newly available version of OpenManage Essentials.
- Warranty scoreboard notification icon  including the number of devices with x days or less of warranty. You can click the icon or number to view the **Device Warranty Report** that lists the device with certain days or less of warranty. The warranty scoreboard notification icon is displayed only if you have selected **Enable Warranty Scoreboard Notifications** in **Settings** → **Warranty Notification Settings**.

In addition to the icons, the banner also contains links to the following:

- **Dell TechCenter** — Click to view the information on various technologies, best practices, knowledge sharing, and information on Dell products.
- **Support** — Click to open Dell.com/support.
- **Help** — Click to open the online help.
- **About** — Click to view general OpenManage Essentials product information.
- **User name** — Displays the user name of the currently logged in user. Move the mouse pointer over the user name to display the following options:
 - **User Info** — Click to view the OpenManage Essentials roles associated with the current user.
 - **Sign in as Different User** — Click to log in to OpenManage Essentials as a different user.

 **NOTE: The Sign in as Different User option is not supported on Google Chrome.**

 **NOTE: The banner is available in all the pages.**

Related links

[Viewing the user information](#)

[Logging in as a different user](#)

[Using the Update Available Notification Icon](#)

[Using the Warranty Scoreboard Notification Icon](#)

Customizing the portals

You can change the layout of the portal page to do the following:

- Display additional available reports.

 **NOTE: This option is only available in the Home portal.**

- Hide graphs and reports.
- Rearrange or resize graphs and reports by dragging and dropping.

If a pop-up window on any screen is bigger than the screen and if scrolling is not possible, set the zoom value of the browser to 75% or less.

From the various reports that are available, you can select specific reports and set them to display on the Dashboard. You can click these reports to get more details. For the list of available reports, see [Home Portal Reports](#).

For more information on the:

- Home portal, see [OpenManage Essentials Home Portal Reference](#).
- Device portal, see [Devices Reference](#).
- Discovery and inventory portal, see [Discovery And Inventory Reference](#).
- Reports portal, see [Reports Reference](#).

Displaying additional reports and graphs

Charts have drill-down feature. To view additional reports and graphs, click the



Figure 2. Adding additional reports and graphs icon

icon on the top right corner. The following list of available reports and graphs is displayed:

- **Alerts by Severity**
- **Devices by Status**
- **Discovered vs. Inventoried Devices**
- **Alerts**
- **Asset Acquisition Information**
- **Asset Maintenance Information**
- **Asset Support Information**
- **ESX Information**
- **FRU Information**
- **Hard Drive Information**
- **HyperV Information**
- **License Information**
- **Memory Information**
- **Modular Enclosure Information**
- **NIC Information**
- **PCI Device Information**
- **Server Components and Versions**
- **Server Overview**
- **Storage Controller Information**
- **Task Status**

After selecting the desired report or graph, dock the report or graph by using the following control to the desired location:

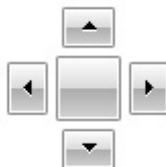


Figure 3. Docking icon

Drilling down charts and reports for more information

To drill-down for further details, perform one of the following:

- In report charts, click the charts.

- In report tables, use the drag and drop option or funnel options to filter the required data and right-click the table rows to perform various tasks.

Saving and loading the portal layout

To save and load the portal layout, click the



Figure 4. Save icon

icon.

All the current layout settings and visible reports on the portal are saved on the portal page.

To load the previous portal layout, click the



Figure 5. Loading the previous portal layout icon.

icon.

Updating the portal data

To refresh the portal page manually, click the



Figure 6. Refresh icon

icon.

To load the default portal layout, click the



Figure 7. Default layout icon

icon.

Hiding graphs and reports—Components

To hide graphs and reports (components), click the



Figure 8. Hide icon

icon on the report or graph and select the **Hide** option to remove the component from the portal page or select the **Auto Hide** option to move the component to the side bar.

To remove a component from the portal page, click the **X** icon in the report or graph.

To move the report to the side bar, click the



Figure 9. Move icon

icon.

Rearranging or resizing graphs and reports—Components

Click the  icon and select from the following options:

- **Floating** — To move the component freely in the portal page.
- **Dockable** — To dock the component in the portal page. If the component is floating, right-click the title to dock or tab the component.
- **Tabbed Document** — To move the component into a tab in the portal page.

Select the

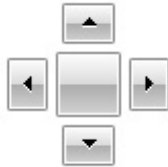


Figure 10. Docking icon.

control to dock a floating component. You can create a tabbed view by docking a pane within other panes or dock a pane at the top, bottom, left, or right side of the main window.

You can resize panes and all panes fill the selected area when docked.

To move the component to the side bar, click the



Figure 11. Move icon

icon and to restore it, select the component and click the



Figure 12. Restore icon

icon.

To create filters in a report grid, click the



Figure 13. Filter icon

icon. This is not specific to the portal page layout and the settings related to these associations are not saved.

Filtering data

You can filter the results by dragging and dropping column headers to the top of reports. You can choose one or more attributes when revising the view to meet your specific needs.

For example, in **Devices by Status** pie chart, click a status such as **Critical**. In the **Device Summary** page, drag the **Device Type** and **Service Tag** to the top of the report. The view immediately changes to a nested information based on your preference. In this example, the information is grouped first by **Device Type**, and second by **Service Tag**. Drill-down through these filtered groups to view the remaining information for the devices.

For more information, see [Viewing Device Summary](#).

Using the Search Bar

The search bar is displayed at the top-right of the dashboard below the heading banner. The search bar is accessible from all portal pages, except when a pop-up or wizard is displayed. As you type text in the search bar, matching or similar item are displayed in the drop-down list.

Related links

- [Searching items](#)
- [Using the search drop-down list](#)
- [Search results and the default actions](#)

Searching items

You can search for the following using the search bar:

- Devices
- Device groups
- Discovery ranges
- Discovery range groups
- Exclude ranges
- Portals
- Wizards
- Remote tasks
- Preferences and settings

When a range, task, device, and so on is changed or created in the console, it is added to the searchable items within 20 seconds.

Related link

- [Using the Search Bar](#)

Using the search drop-down list

The search bar displays a list as you type text in the search box. The items that contain the characters that you type are populated in the search drop-down list. Each item in the drop-down list includes two icons and the name of the item. The first icon indicates the item category (such as **Device**, **Launch Wizard**, and so on). The second icon indicates the state of the item (such as **Normal**, **Critical**, or **Warning**). Immediately after the two icons, the name of the item is displayed. Moving the mouse pointer over an item in the drop-down list, displays a tool tip. The information displayed in the tool tip varies based on the item. For example, moving the mouse pointer over a device displays the following: **Name**, **Type**, **Health Status**, **Power Status**, **IP Address**, **Service Tag**, and **MAC Address**. Selecting an item displayed in the tool tip performs the default action.

Related link

- [Using the Search Bar](#)

Search results and the default actions

Selecting or clicking an item displayed in the search bar results in the following default actions:


Table 5. Selection Actions

Item Selected	Action
Devices	Displays the device details.
Device Groups	Displays the device group summary.
Discovery Ranges	Displays the discovery range.
Discovery Range Group	Displays the discovery range group summary.
Portals	Navigates to the appropriate portal.
Wizards	Launches the appropriate wizard.
Exclude Range	Displays the range summary.
Remote Tasks	Selects a task in the task tree.


Related link

[Using the Search Bar](#)

Map View—Home Portal

 **NOTE:** The Map View feature is available only if you have discovered any PowerEdge VRTX or PowerEdge FX2/FX2s devices that have an Enterprise license using the WS-Man protocol. If the licensed device is discovered using the SNMP protocol, the Map View feature is not available. In this case, you must rediscover the device using the WS-Man protocol.

The **Map View** (home) portal can be accessed by clicking the **Map View** link in the **Home** portal.

 **NOTE:** You can also access another implementation of the map (Map View tab) that is accessible through the **Devices** portal.

The following are the features of the **Map View** (home) portal:

- The **Map View** (home) portal is not integrated with the device tree.
- You can select a device group to display on the map by using the **Filter by** drop-down box at the top of the map.
- Clicking a pin (device) on the **Map View** (home) portal opens the **Devices** portal that displays details about the device.
- Any change to the devices or settings on the **Map View** (home) portal is synchronized with the **Map View** tab accessible through the **Devices** portal.
- Zoom level and the visible portion of the **Map View** (home) portal are not synchronized with the **Map View** tab accessible through the **Devices** portal.

 **NOTE:** For information about using the features available in Map View, see [Using Map View](#).

Related links

[Using the OpenManage Essentials Home Portal](#)

[Map View Interface—Home Portal](#)

Viewing the user information

To view the user information such as the OpenManage Essentials roles associated with the current user:

1. Move the mouse pointer over the user name in the heading banner.
2. In the menu that is displayed, click **User Info**.
The **User Information for <user name>** dialog box with the user information is displayed.

Related link

[OpenManage Essentials Heading Banner](#)

Logging in as a different user

 **NOTE:** The Sign in as Different User option is not displayed on Google Chrome and Mozilla Firefox browsers. To log in as a different user when using Chrome or Firefox, close and reopen the browser, provide the new user credentials when prompted, and click OK.

 **NOTE:** When using the Sign in as Different User option in Internet Explorer, you may be prompted to provide the credentials multiple times

To log in as a different user:

1. Move the mouse pointer over the user name in the heading banner.
2. In the menu that is displayed, click **Sign in as Different User**.
The **Windows Security** dialog box is displayed, prompting for the user name and password.
3. Type the **User name** and **Password**, and click **OK**.


Related links

[Using the OpenManage Essentials Home Portal](#)
[OpenManage Essentials Heading Banner](#)

Using the Update Available Notification Icon

 **NOTE:** The update available notification icon may be displayed in the OpenManage Essentials heading banner only after you refresh the web browser.


The update available notification icon  is displayed in the OpenManage Essentials heading banner when a new version of

OpenManage Essentials is available. Click the  icon to open the **New Version Available** window that displays the currently installed and newly available version of OpenManage Essentials. You can click **Learn More** to view the download details on the OpenManage Essentials website. Click **Remind Me Later** to set or cancel the update available notification.

Related link

[OpenManage Essentials Heading Banner](#)

Using the Warranty Scoreboard Notification Icon

The warranty scoreboard notification icon  is displayed in the OpenManage Essentials heading banner based on the criteria you have configured in **Settings** → **Warranty Notification Settings**. The warranty scoreboard notification also displays the number of

devices that meet the criteria you have configured. Click the  icon to display the **Device Warranty Report** that provides the warranty information of devices based on your **Warranty Scoreboard Notifications** settings.

Related links

[OpenManage Essentials Heading Banner](#)
[Configuring Warranty Scoreboard Notifications](#)
[Device Warranty Report](#)

OpenManage Essentials Home Portal — Reference

Related links

[OpenManage Essentials Heading Banner](#)
[Dashboard](#)
[Schedule View](#)
[Using the Search Bar](#)
[Map View Interface—Home Portal](#)

Dashboard

The dashboard page provides a snapshot of the managed devices that include servers, storage, switches, and so on. You can filter the view based on the devices by clicking the **Filter by:** drop-down list. You can also add a new group of devices from the dashboard by clicking **Add New Group** from the **Filter by:** drop-down list.

Related links

[Using the Search Bar](#)
[Discovered Versus Inventoried Devices](#)
[Task Status](#)
[Home Portal Reports](#)
[Device by Status](#)
[Alerts by Severity](#)

Home Portal Reports

From the Home Portal Dashboard page, you can monitor the following:

- **Alerts by Severity**
- **Devices by Status**
- **Discovered vs. Inventoried Devices**
- **Alerts**
- **Asset Acquisition Information**
- **Asset Maintenance Information**
- **Asset Support Information**
- **ESX Information**
- **FRU Information**
- **Hard Drive Information**
- **HyperV Information**
- **License Information**
- **Memory Information**
- **Modular Enclosure Information**
- **NIC Information**
- **PCI Device Information**
- **Server Components and Versions**
- **Server Overview**
- **Storage Controller Information**

- Task Status

Device by Status

Device by Status provides device status information in a pie chart format. Click a segment of the pie chart to view the device summary.

Table 6. Device by Status

Field	Description
Unknown	Health status of these devices are not known.
Normal	Devices are working as expected.
Warning	These devices display behaviors that are not normal and further investigation is required.
Critical	These devices display behaviors that suggest an occurrence of a failure of a very important aspect.
Connection Lost	These devices are not reachable.

Alerts by Severity

Alerts by severity provide alert information of devices in a pie chart format. Click a segment of the pie chart to view the devices.

Table 7. Alerts by Severity

Field	Description
Unknown	Health status of these devices are not known.
Normal	Alerts from these devices conform to the expected behavior for the devices.
Warning	These devices display behaviors that are not normal and further investigation is required.
Critical	Alerts from these devices suggest that a failure of a very important aspect has occurred.

Discovered Versus Inventoried Devices

The graph displays the number of devices and servers discovered or inventoried. You can use this report to ascertain the discovered devices and servers that are unclassified. For more information on the filter options for the summary information, see [Viewing Device Summary](#).

Click any section of the graph to view the **Device Summary** for the selected region. In the device summary, double-click a row to view the details (inventory view for that device). Alternatively, right-click and select details for the inventory view or right-click and select alerts for the alerts specific to that device.

Table 8. Discovered Versus Inventoried Devices

Field	Description
Filter by	Select to filter the search results using the following options: <ul style="list-style-type: none"> All Ranges — Select to filter based on the selected range.

Related links

- [Creating a discovery and inventory task](#)
- [Viewing configured discovery and inventory ranges](#)
- [Excluding ranges](#)
- [Scheduling discovery](#)
- [Scheduling inventory](#)
- [Configuring status polling frequency](#)
- [Discovery and Inventory Portal](#)

Task Status

The grid provides a list of currently executing and previously run tasks and their status. The **Task Status** grid on this page shows the status of just discovery, inventory, and tasks. However, the main portal shows all types of task statuses.

Related links

- [Creating a discovery and inventory task](#)
- [Viewing configured discovery and inventory ranges](#)
- [Excluding ranges](#)
- [Scheduling discovery](#)
- [Scheduling inventory](#)
- [Configuring status polling frequency](#)
- [Discovery and Inventory Portal](#)

Schedule View

From **Schedule View** you can:

- View tasks that are scheduled to occur and tasks that are completed.
- Filter the view based on the type of task (such as database maintenance tasks, server power options, and so on), active tasks, and task execution history.




NOTE: The options displayed in the Filter by drop-down list vary depending on the tasks that are created. For example, if a Server Options Task is not created, then the option is not displayed in the Filter by drop-down list.

- View tasks for a particular day, week, or month. You can also view the tasks for a particular day by clicking the calendar icon.
- Drag and drop tasks to a time slot in the calendar.
- Set the zoom value by changing the zoom slider.



NOTE: The zoom slider is disabled for the Month view.

- Export the schedules to a .ics file and import the file into Microsoft Outlook.

- Change the schedule view settings by clicking the settings icon  .

For more information, see [Schedule View Settings](#).


Related link

- [Schedule View Settings](#)

Schedule View Settings

Table 9. Schedule View Settings

Field	Description
Orientation	Allows you to change the orientation of the Schedule View page and the displayed tasks. You can select either the Vertical or Horizontal orientation.

Field	Description
	 NOTE: Changing the Orientation setting does not affect the Month view.
Schedule Item Size	Allows you to modify the size of the tasks displayed.
Color Categorize by Task Type	Selecting this option categorizes each task type using a different color.
Show Task Execution History	Select this option to display the tasks that are already complete.
Show Database Maintenance	Select this option to view the time at which database maintenance occurs.

Device Warranty Report


The **Device Warranty Report** is displayed when you click the warranty scoreboard notification icon  on the OpenManage Essentials heading banner. The following are the fields displayed in the **Device Warranty Report**.

Table 10. Device Warranty Report

Field	Description
All Devices with x days or less of warranty	Determines which devices to include in the Device Warranty Report . Devices with warranty less than or equal to the specified days are included in the warranty report.
Include Expired Warranties	Specifies if devices with expired warranty (0 days) or no warranty information should be included in the warranty email notification.
Preview	Displays the warranty report based on the criteria set in All Devices with x days or less of warranty .
OK	Closes and saves any changes made to the Device Warranty Report .
View and Renew Warranty	Displays a link you can click to open the Dell website from where you can view and renew the device warranty.
Device Name	Displays the system name that is unique and identifies the system on the network.
Model	Displays the model information of the system.
Device Type	Displays the type of device. For example, server or Remote Access Controller.
Service Tag	Displays the specific unique bar code label identifier for the system.
Service Level Code	Displays the service level code such as parts only warranty (POW), next business day onsite (NBD), and so on for a particular system.
Warranty Type	Displays the warranty type. For example, initial, extended, and so on.
Warranty Description	Displays the warranty details applicable for the device.
Service Provider	Displays the name of the organization that will provide the warranty service support for the device.
Shipped Date	Displays the date on which the device was shipped from the factory.
Start Date	Displays the date from which the warranty is available.

Field	Description
End Date	Displays the date on which the warranty will expire.
Days Remaining	Displays the number of days the warranty is available for the device.

Related links

[Using the Warranty Scoreboard Notification Icon](#)

[Configuring Warranty Scoreboard Notifications](#)

Map View Interface—Home Portal

The **Map View** (home) portal accessible through the **Home** portal has a **Filter by** drop-down list which you can use to filter the device group displayed on the map. The menus and options available in the **Map View** (home) portal are the same as those found in the **Map View** tab in the **Devices** portal. For information about the menus and options in the **Map View**, see [Map View \(Devices\) Tab Interface](#).

Related link

[Map View—Home Portal](#)

Discovering and inventorying devices

Perform discovery and inventory to manage your network devices.

Related links

[Creating a discovery and inventory task](#)

[Viewing configured discovery and inventory ranges](#)

[Scheduling discovery](#)

[Scheduling inventory](#)

[Excluding ranges](#)

[Supported devices, protocols, and features matrix—SNMP, WMI, and WS-Man](#)



Supported devices, protocols, and features matrix—SNMP, WMI, and WS-Man


 **NOTE:** For description of the features listed in the following table, see [Legend and Definitions](#).

Table 11. Supported devices, protocols (SNMP, WMI, WS-Man), and features matrix

Protocol / Mechanism		Simple Network Management Protocol (SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management (WS-Man)	REpresentational State Transfer (REST)
Servers with OpenManage Server Administrator installed	Windows / Hyper-V	Discovery Correlation Classification Hardware inventory Software inventory Monitoring Traps/alerts Application launch <ul style="list-style-type: none"> OpenManage Server Administrator console RAC Remote desktop System update 	Discovery Correlation Classification Hardware inventory Software inventory Monitoring Application launch <ul style="list-style-type: none"> OpenManage Server Administrator console Remote desktop System update 	Not supported	Not supported
	Linux/ VMware ESX	Discovery Correlation Classification Hardware inventory Software inventory Monitoring Traps/alerts Application launch <ul style="list-style-type: none"> OpenManage Server 	Not supported	Not supported	Not supported


Protocol / Mechanism		Simple Network Management Protocol (SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management (WS-Man)	REpresentational State Transfer (REST)
		Administrator console • RAC			
	VMware ESXi	Traps/alerts	Not supported	Discovery Correlation Classification Hardware inventory Software inventory Virtual machine information Virtual host product information Monitoring (OpenManage Server Administrator health only) Application launch—RAC	Not supported
Servers without OpenManage Server Administrator installed	Windows/Hyper-V	Not supported	Discovery Correlation Classification Hardware inventory Application launch • Remote desktop	Not supported	Not supported
	Linux/VMware ESX	Not supported	Not supported	Not supported	Not supported
	VMware ESXi	Not supported	Not supported	Discovery Correlation Classification Hardware inventory (no storage inventory) Application launch	Not supported
iDRAC / DRAC / BMC		Discovery Correlation Classification Monitoring Traps/ Platform Event Traps (PET) Application launch • RAC • Console	Not supported	Discovery Correlation Classification Monitoring Traps/ Platform Event Traps (PET) Hardware inventory System update	Not supported


Protocol / Mechanism	Simple Network Management Protocol (SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management (WS-Man)	REpresentational State Transfer (REST)
			 NOTE: Applicable only to iDRAC6 version 1.3 and later. Discovery and hardware inventory are not supported for iDRAC6 version 1.25 and earlier. Application launch <ul style="list-style-type: none"> • RAC • Console 	
Hyper-Converged Infrastructure (VxRail, XC Series)	Discovery Correlation Classification Monitoring Traps/ Platform Event Traps (PET) Application launch <ul style="list-style-type: none"> • RAC • Console 	Not supported	Discovery Correlation Classification Monitoring Traps/ Platform Event Traps (PET) Hardware inventory Application launch <ul style="list-style-type: none"> • RAC • Console • VxRail Manager • PRISM  NOTE: OpenManage Essentials does not support remote task execution, server configuration, and system updates on the VxRail and XC Series devices.	Not supported
Modular enclosure (PowerEdge M1000e)	Discovery Correlation Classification Enclosure health Traps System update Application launch— CMC	Not supported	Discovery Correlation Classification Enclosure health Traps System update Application launch— CMC	Not supported


Protocol / Mechanism	Simple Network Management Protocol (SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management (WS-Man)	REpresentational State Transfer (REST)
			 NOTE: Applicable only to PowerEdge M1000e with CMC firmware version 5.0.	
Modular enclosure (PowerEdge MX7000)	Traps	Not supported	Not supported	Discovery Correlation Classification Enclosure health Traps System update Application launch— OpenManage Enterprise - Modular
PowerEdge VRTX	Discovery Correlation Classification Enclosure health Traps Application launch— CMC	Not supported	Discovery Correlation Classification Hardware inventory System Update Enclosure health Traps Application launch— CMC Map View (PowerEdge VRTX only)	Not supported
Networking W-Series Mobility Controllers and Access Points	Discovery Inventory Classification Application launch Traps/alerts Health—active and inactive Switch Role	Not supported	Not supported	Not supported
SonicWALL firewall appliances	Discovery Classification Application launch Traps/alerts	Not supported	Not supported	Not supported
Networking Ethernet switches	Discovery Correlation Classification Application launch Traps/alerts Health Switch Role	Not supported	Not supported	Not supported
Brocade Fibre Channel switches	Discovery	Not supported	Not supported	Not supported

Protocol / Mechanism	Simple Network Management Protocol (SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management (WS-Man)	REpresentational State Transfer (REST)
	Classification Application launch Traps/alerts Health Switch role			
VxFlex Ready Nodes	Discovery Correlation Classification Monitoring Traps/ Platform Event Traps (PET) Application launch— VxFlex Ready Node Series Support	Not supported	Discovery Correlation Classification Monitoring Traps/ Platform Event Traps (PET) Hardware inventory System update Application launch— VxFlex Ready Node Series Support	Not supported

 **NOTE:** For full functionality of chassis support in OpenManage Essentials, the chassis and the associated devices must be discovered using the appropriate protocols.

 **NOTE:** OpenManage Essentials supports in-band (OMSA) and out-of-band (iDRAC) discovery of the following PowerEdge C-Series servers only: PowerEdge C4130, PowerEdge C6320, PowerEdge C6320p, and PowerEdge C6420.

 **NOTE:** OpenManage Essentials supports discovery of Dell Precision Rack 7910 and 7920 clients with WMI protocol similar to the discovery of other client devices. If the Dell Precision Rack 7910 and 7920 clients are discovered using iDRAC (out-of-band discovery), then these devices are classified as Servers under Manage → Devices → All Devices → RAC.

 **NOTE:** You can also perform discovery and inventory of a server out-of-band (iDRAC) using the credentials of the iDRAC user account that has Read Only privileges. However, you cannot perform operations that require elevated privileges such as system update, device configuration deployment, and so on.

Supported devices, protocols, and features matrix—IPMI, CLI, and SSH

 **NOTE:** For description of the features that are listed in the following table, see [Legend and Definitions](#).


Table 12. Supported devices, protocols (IPMI, CLI, SSH), and features matrix

Protocol / Mechanism		Intelligent Platform Management Interface (IPMI)	Command Line Interface (CLI) ^a	Secure Shell (SSH)
Servers with OpenManage Server Administrator installed	Windows /Hyper-V	Not supported	OpenManage Server Administrator CLI Deploy OpenManage Server Administrator Server Updates • BIOS • Firmware	Not supported

Protocol / Mechanism		Intelligent Platform Management Interface (IPMI)	Command Line Interface (CLI) ^a	Secure Shell (SSH)
			<ul style="list-style-type: none"> Driver 	
	Linux/ VMware ESX	Not supported	OpenManage Server Administrator CLI Deploy OpenManage Server Administrator Server Updates <ul style="list-style-type: none"> BIOS Firmware Driver 	Discovery Correlation Classification Hardware and Software Inventory (minimal)
	VMware ESXi	Not supported	Not supported	Discovery Correlation Classification Hardware and Software Inventory (minimal)
	XenServer	Not supported	RACADM CLI IPMI CLI OpenManage Server Administrator CLI Power Task	Not supported
Servers without OpenManage Server Administrator installed	Windows/Hyper-V	Not supported	Deploy OpenManage Server Administrator	Not supported
	Linux/VMware ESX	Not supported	Deploy OpenManage Server Administrator	Discovery Correlation Classification Hardware and Software Inventory (minimal)
	VMware ESXi	Not supported	Not supported	Not supported
	PowerEdge C	Discovery Classification	RACADM CLI IPMI CLI	Not supported
iDRAC / DRAC / BMC		Discovery Classification Correlation iDRAC health	RACADM CLI IPMI CLI	Not supported
Modular Enclosure (M1000e) / PowerEdge VRTX / PowerEdge FX		Not supported	RACADM CLI IPMI CLI	Not supported
Modular Enclosure (PowerEdge MX7000)		Not supported	RACADM CLI	Not supported
Networking W-Series Mobility Controllers and Access Points		Not supported	Not supported	Not supported
SonicWALL firewall appliances		Not supported	Not supported	Not supported
Networking Ethernet switches		Not supported	Not supported	Not supported
Brocade Fibre Channel switches		Not supported	Not supported	Not supported
VxFlex Ready Nodes		Discovery Classification	RACADM CLI IPMI CLI	Not supported

Protocol / Mechanism	Intelligent Platform Management Interface (IPMI)	Command Line Interface (CLI) ^a	Secure Shell (SSH)
	Correlation iDRAC health		

a) You cannot perform this task if the device is not discovered, inventoried, or both.



 **NOTE:** Correlation of PowerEdge FC430, FC630, or FC830 sleds under the host chassis is not supported in the following scenarios:

- The sleds are discovered using WMI protocol (in-band) and do not have OMSA installed.
- The sleds are discovered using IPMI protocol (out-of-band).
- The sleds are running ESXi and either have or do not have OMSA installed.

Supported storage devices, protocols, and features matrix

 **NOTE:** For description of the features listed in the following table, see [Legend and Definitions](#).

Table 13. Supported storage devices, protocols, and features matrix

Protocol / Mechanism		Simple Network Management Protocol (SNMP)	Symbol	EMC Navisphere CLI
Storage Devices	Dell EqualLogic	Discovery Classification Hardware inventory Monitoring Traps/alerts Application launch — EqualLogic console  NOTE: It is recommended that you discover EqualLogic storage arrays using the Group Management IP or Storage Group IP only, and not include any of the member IPs in the discovery range configuration.	Not supported	Not supported
	Dell EMC  NOTE: Both SNMP and Navisphere are required for complete management of Dell EMC devices.	Discovery Classification Traps/Alerts	Not supported	Hardware inventory Monitoring Application launch — EMC Navisphere Manager
	PowerVault	Traps/Alerts	Discovery	Not supported

Protocol / Mechanism		Simple Network Management Protocol (SNMP)	Symbol	EMC NaviSphere CLI
			Classification Hardware inventory Monitoring Application launch — Modular Disk Storage Manager (a)	
	Compellent	Discovery Classification Hardware inventory Monitoring Traps/alerts Application launch — Compellent console	Not supported	Not supported
	Tape	Discovery Classification Hardware inventory Monitoring Traps/alerts Application launch — Tape console	Not supported	Not supported

a) Requires Modular Disk Storage Manager Controller software installed on the OpenManage Essentials system.

 **NOTE: Storage devices hosted by the PowerEdge M1000e chassis are not classified under the Storage node of the chassis until the PowerEdge M1000e chassis is inventoried.**

 **NOTE: When an EqualLogic group that is associated with a NAS appliance is discovered, the EqualLogic group is displayed in the device tree under NAS Clusters and Storage Devices → Dell EqualLogic Groups. However, the members of the EqualLogic group are displayed only under Dell EqualLogic Groups.**

Setting up and configuring VMware ESXi 5

 **NOTE: Before setting up and configuring VMware ESXi 5, ensure that you have ESXi 5 build 474610 or later. If you do not have the required build, download the latest build from vmware.com.**

To set up and configure VMware ESXi 5:

1. Download the latest version (7.4) of OpenManage offline bundle for ESXi from Dell.com/support.
2. If you have enabled SSH, copy the file using WinSCP or a similar application to the `/tmp` folder on the ESXi 5 host.
3. Using Putty, change permissions on the OpenManage offline bundle for ESXi file using the command `chmod u+x <Dell OpenManage version 7.4 offline bundle for ESXi file name>.zip`.

 **NOTE: You can also change permissions using WinSCP.**

4. Run the following commands using:

- Putty — `esxcli software vib install -d /tmp/<Dell OpenManage version 7.4 VIB for ESXi file name>.zip`
- VMware CLI — `esxcli -server <IP Address of ESXi 5 Host> software vib install -d /tmp/<Dell OpenManage version 7.4 VIB for ESXi file name>.zip`

The message `VIBs Installed: Dell_bootbank_OpenManage_7.4-0000` is displayed.

5. Restart the host system.
6. After restarting, verify if OpenManage is installed by running the following commands using:

- Putty — `esxcli software vib list`
 - VMware CLI — `esxcli -server <IP Address of ESXi 5 Host> software vib list`
7. Configure SNMP, for hardware alerts on the ESXi 5 host, to send SNMP traps to OpenManage Essentials. SNMP is not used for discovery. WS-Man is required for discovery and inventory of an ESXi 5 host. To group the VMs with the ESXi host in the OpenManage Essentials device tree after you discover the VM, SNMP must be enabled on the ESXi host and the VM.
 8. Create a discovery range and configure WS-Man.
For more information on setting up and configuring ESXi 5, see the *How to setup and configure ESXi 5 for use in OME* technical white paper at DellTechCenter.com/OME.

Legend and definitions

- **Discovery:** Capability to discover the devices on the network.
- **Correlation:** Capability to correlate:
 - CMC with servers, switches, RAC, and storage.
 - Discovered server and DRAC, iDRAC, or BMC devices.
 - Discovered modular systems or switches.
 - ESX, ESXi, or Hyper-V host and guest virtual machines.
- **Classification:** Capability to classify the devices by type. For example, servers, network switches, storage, and so on.
- **Hardware Inventory:** Capability to obtain detailed hardware inventory of the device.
- **Monitoring or Health:** Capability to obtain health status and connection status of the device.
- **Traps, alerts, or PETs:** Capability to receive SNMP traps from the device.
- **Application Launch:** Provides a right-click action menu item on the discovered device to launch 1x1 console or application.
- **OpenManage Server Administrator CLI:** Capability to run OpenManage Server Administrator supported commands on the remote (discovered) servers.
- **Deploy OpenManage Server Administrator:** Capability to deploy OpenManage Server Administrator to the remote (discovered) servers.
- **Server Updates:** Capability to deploy BIOS, firmware, and driver updates to the remote (discovered) servers.
- **RACADM CLI:** Capability to run RACADM tool supported commands on the remote (discovered) devices.
- **IPMI CLI:** Capability to run IPMITool supported commands on the remote (discovered) devices.
- **Switch Role:** Indicates the type of the unit, such as management or stack.

Using the Discovery and Inventory Portal

To access the discovery and inventory portal, click **Manage** → **Discovery and Inventory**.

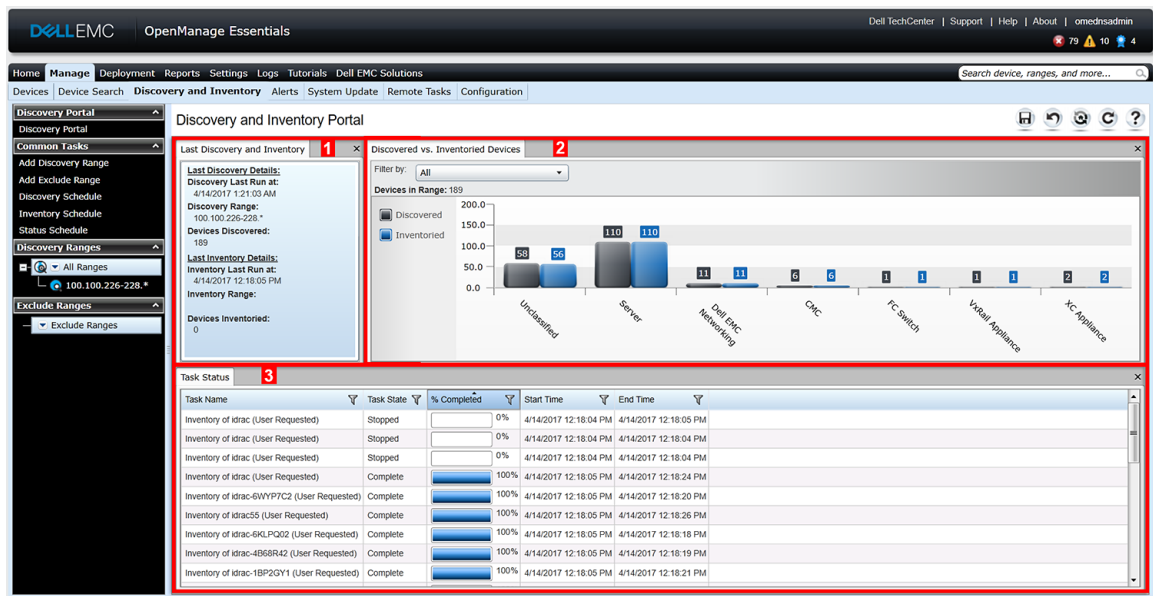


Figure 14. Discovery and Inventory Portal

1. Details from the last discovery and inventory task run.
2. Details of previously discovered and inventoried devices.
3. Details of tasks and their status.

Protocol support matrix for discovery

The following table provides information about the supported protocols for discovering devices. The recommended protocol is indicated by the text in *italics*.

Table 14. Protocol support matrix for discovery

Device/ Operating System	Protocols					
	Simple Network Management Protocol (SNMP)	Web Services- Management (WS-Man)	Windows Management Instrumentatio n (WMI)	Intelligent Platform Management Interface (IPMI)	Secure Shell (SSH)	REpresentational State Transfer (REST)
iDRAC6, or later	Supported	<i>Supported</i>	N/A	Supported	Not supported	N/A
Linux	<i>Supported</i> ¹	N/A	N/A	N/A	Supported	N/A
Windows	<i>Supported</i> ¹	N/A	Supported ²	N/A	N/A	N/A
ESXi	Supported ¹	<i>Supported</i>	N/A	N/A	Not supported	N/A
Citrix XenServer	<i>Supported</i> ¹	N/A	N/A	N/A	Supported ²	N/A
PowerEdge (CMC)	Supported	<i>Supported</i>	N/A	N/A	Not supported	N/A
PowerEdge MX7000	Not supported	N/A	N/A	N/A	Not supported	<i>Supported</i>
PowerEdge C*	Supported	Supported	N/A	<i>Supported</i>	Not supported	N/A
Client systems	Supported ³	N/A	<i>Supported</i> ³	N/A	N/A	N/A
Storage devices	Supported	N/A	N/A	N/A	N/A	N/A

Device/ Operating System	Protocols					
	Simple Network Management Protocol (SNMP)	Web Services- Management (WS-Man)	Windows Management Instrumentatio n (WMI)	Intelligent Platform Management Interface (IPMI)	Secure Shell (SSH)	REpresentational State Transfer (REST)
Ethernet switches	Supported	N/A	N/A	N/A	N/A	N/A

* Discovery of PowerEdge C4130, PowerEdge C6320, PowerEdge C6320p and PowerEdge C6420 can be performed using the same protocols that are used to discover any other non C-Series PowerEdge servers.

¹ Supported with OpenManage Server Administrator (OMSA) installed.

² Supported with OMSA installed; no health information without OMSA.

³ Supported with Dell Command | Monitor installed; no health information without Dell Command | Monitor.

Protocol support matrix for system update

The following table provides information about the supported protocols for the system update tasks. The recommended protocol is indicated by the text in *italics*.

Table 15. Protocol support matrix for system update

Device/ Operating System	Protocols					
	Simple Network Management Protocol (SNMP)	Web Services- Management (WS-Man)	Windows Management Instrumentation (WMI)	Intelligent Platform Management Interface (IPMI)	Secure Shell (SSH)	REpresentational State Transfer (REST)
iDRAC6, or later	Not supported	<i>Supported</i>	N/A	N/A	N/A	N/A
Linux	<i>Supported</i> ¹	N/A	N/A	N/A	Supported ²	N/A
Windows	<i>Supported</i> ¹	N/A	Supported ^{1,2}	N/A	N/A	N/A
ESXi	Not supported	<i>Supported</i> ³	N/A	N/A	N/A	N/A
Citrix XenServer	Not supported	N/A	N/A	N/A	N/A	N/A
PowerEdge (CMC)	Supported ⁴	<i>Supported</i> ⁴	N/A	N/A	N/A	N/A
PowerEdge MX7000	Not supported	N/A	N/A	N/A	Not supported	<i>Supported</i>

¹ Supported with OpenManage Server Administrator (OMSA) installed.

² Supported using the inventory collection method.

³ Supported; requires iDRAC to be discovered and updated through out-of-band channel.

⁴ Supported; requires the RACADM tool.

Devices not reporting Service Tag

Service Tag is not displayed in the OpenManage Essentials console for the following devices:


- KVM
- Dell PowerVault 132T
- PowerVault 136T
- PowerVault ML6000


- Dell Networking W-Series Mobility Controllers
- Dell SonicWALL Firewall appliances (global health status is also not available)
- Printers
- PDU
- UPS

 **NOTE:** Due to lack of Service Tag information, the warranty information of these devices is not available.

Creating a discovery and inventory task

1. From OpenManage Essentials, click **Manage** → **Discovery and Inventory** → **Common Tasks** → **Add Discovery Range**.
The **Discover Devices** wizard is displayed. The type of wizard displayed is based on the configuration in **Settings** → **Discovery Settings**. See [Configuring Discovery Settings](#).
2. In **Discovery Range Configuration**:
 - a. If you want to create a range group, select **Save as Group**, and provide the **Group Name**.
 - b. Enter the IP address/range or the host name and subnet mask, and then click **Add**.

 **NOTE:** You can add multiple IP addresses, ranges, or host names. You can add multiple host names separated by a comma delimiter. For example, `hostname1, hostname2, hostname3`, and so on.
 - c. To import host names and IP addresses, click **Import**. You can also import host names and IP addresses included as line items in .csv file. Using Microsoft Excel, you can create a .csv file containing host names or IP addresses.

 **NOTE:** The discovery range can be exported as a .csv file by right-clicking **All Ranges** or a given discovery range. The exported .csv file with the host names and IP addresses can be imported in the same or a different OpenManage Essentials instance.
 - d. Click **Next**.
3. If you have selected the **Standard Wizard** in [Discovery Settings](#) — After you have provided at least one IP address, IP range, host name, or a combination thereof, continue to customize the discovery and inventory options or complete the configuration using the default options. Clicking **Finish** without setting any further configurations immediately runs the discovery and inventory tasks by using the default SNMP and ICMP protocols. It is recommended that you review and revise your protocol configurations prior to clicking **Finish**.

For more information about each listed protocol, click the help icon  in the appropriate protocol configuration screen.

 **NOTE:** When discovering ESXi-based servers, to view the guest virtual machines grouped with the host, enable and configure the WS-Man protocol.

 **NOTE:** By default, SNMP is enabled and values are assigned ICMP parameters.


 **NOTE:** ICMP ping is optional for OpenManage Essentials version 2.4 and later. The ICMP parameters are applied depending on the selection of **Skip ICMP ping** during discovery setting.

 **NOTE:** After completing any of the following steps, click either **Next** to continue or click **Finish** to complete the **Discovery Range Configuration**.

- In **ICMP Configuration**, to detect devices on the network, edit the ICMP parameters.

 **NOTE:** The ICMP Configuration window is not displayed if **Skip ICMP ping** during discovery setting is selected under **Settings** → **Discovery Settings**.

- In **SNMP Configuration**, to discover servers, provide the SNMP parameters. You can select SNMP V1/V2c or SNMP V3 for discovery. Ensure that the SNMP community string specified in **Get Community** matches the SNMP community string of the device or devices you want to discover using SNMP V1/V2c. For discovery and inventory of the devices using SNMP V3, ensure the devices are configured with same username and password, authentication protocol, and encryption protocol credentials, that is used when discovering the devices.

 **NOTE:** If the user selects both **SNMPv1/v2c** and **SNMPv3** options, then the discovery of devices using **SNMPv3** takes higher priority than discovery of devices using **SNMPv1/v2c**. The **Discovery Range Configuration Details** displays the discovery protocol selected for a particular discovery range.



NOTE: iDRAC supports only the default SNMP port 161. If the default SNMP port is changed, iDRAC may not get discovered.

- In **WMI Configuration**, to authenticate and connect to remote devices, provide the WMI parameters. The format for entering credentials for WMI must be *domain\user name* for domain-based networks or *localhost\user name* for non-domain based networks.
 - In **Storage Configuration**, to discover PowerVault modular disk array or EMC devices, edit parameters.
 - In **WS-Man Configuration**, to enable discovery of PowerEdge VRTX, iDRAC 6, iDRAC 7, ESXi installed servers, and VxFlex Ready nodes, provide WS-Man parameters.
 - In **REST Configuration**, to enable discovery of MX7000 chassis, provide REST parameters. In a Multi-Chassis Management (MCM) group, provide the REST parameters of lead MX7000 chassis.
 - In **SSH Configuration**, to enable discovery of Linux-based servers, provide SSH parameters.
 - In **IPMI Configuration**, to enable server discovery, provide IPMI parameters. IPMI is typically used to discover BMC or iDRACs on servers. You can include the optional KG key when discovering RAC devices.
 - In **Discovery Range Action**, choose to discover, inventory, or perform both tasks. The default option is to perform both discovery and inventory.
 - Select **Perform only discovery** or **Perform both discovery and inventory** to run the task immediately.
 - To schedule the task to run at a later time, select **Do not perform discovery or inventory**, and follow the instructions in [Scheduling Discovery](#) and [Scheduling Inventory](#).
4. If you have selected the **Guided Wizard** option in [Discovery Settings](#) — After you have provided at least one IP address, IP range, host name, or a combination thereof, click **Next**. The **Device Type Filtering** window is displayed. See [Device Type Filtering](#).
 - a. Select the device types that you want to discover and manage.
The required protocols for discovering the selected devices are added to the **Discover Devices** wizard.
 - b. Provide the configuration details for all the protocols listed in the wizard and click **Next**.
 5. Review your selections in the Summary screen and click **Finish**. To change any of the parameters in previous configuration screens, click **Back**. When complete, click **Finish**.

Related links

[Discovery and Inventory Portal](#)
[Last Discovery and Inventory](#)
[Discovered Versus Inventoried Devices](#)
[Task Status](#)

Changing the default SNMP port

SNMP uses the default UDP port 161 for general SNMP messages and UDP port 162 for SNMP trap messages. If these ports are being used by another protocol or service, you can change the settings by modifying the local services file on the system.



NOTE: This section requires Support V1/V2c Traps to be selected in the SNMP Listener Settings under Settings → Alert Settings.

To configure the managed node and OpenManage Essentials to use a non-default SNMP port:

1. In both the management station and managed node, go to **C:\Windows\System32\drivers\etc**.
2. Open the Windows SNMP **services** file using Notepad and edit the following:
 - Incoming SNMP trap port (receiving alerts in OpenManage Essentials) — Modify the port number in the line, `snmptrap 162/udp snmp-trap #SNMP trap`. Restart the SNMP trap service and SNMP service after making the change. On the management station, restart the DSM Essentials Network Monitor service.
 - Outgoing SNMP requests (Discovery/inventory in OpenManage Essentials) — Modify the port number in the line `snmp 161/udp #SNMP`. Restart the SNMP service after making the change. On the management station, restart the DSM Essentials Network Monitor service.
3. Outgoing trap port — In OpenManage Essentials trap forwarding alert action, specify the `<<trap destination address: port number>>` in the **Destination** field.



NOTE: If you have previously configured IP security to encrypt SNMP messages on the default ports, update the IP security policy with the new port settings.

Discovering and inventorying devices by using WS-Man or REST protocol with a root certificate

Before you begin, ensure that the root CA server, OpenManage Essentials management server, and WS-Man or REST target(s) are able to ping each other by hostname.

To discover and inventory Dell EMC devices by using the WS-Man or REST protocol with a root certificate:

1. Open the web console of the target device—iDRAC, CMC, or OpenManage Enterprise Modular (OME - Modular).
2. Generate a new certificate signing request file:
 - a. For iDRAC or CMC, click **Network** and click **SSL**.
For OME - Modular, click **Application Settings** → **Security** → **Certificates**.
 - b. Select **Generate a New Certificate Signing Request (CSR)** and click **Next**.
The **Generate Certificate Signing Request (CSR)** page is displayed.
 - c. If applicable, type the appropriate information in the required fields. Ensure that the **Common Name** is the same as the host name used to access the web console of the device, and then click **Generate**.
 - d. When prompted, save the **request.csr** file.
3. Open the **Microsoft Active Directory Certificate Services – root CA** web server: **http://signingserver/certsrv**.
4. Under **Select a task**, click **Request a certificate**.
The **Request a Certificate** page is displayed.
5. Click **advanced certificate request**.
The **Advanced Certificate Request** page is displayed.
6. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.
7. Using a text editor, open the certificate signing request (.csr or .txt) file you saved in step 2 d.
8. Copy the contents from the certificate signing request file and paste it in the **Saved Request** field.
9. In the **Certificate Template** list, select **Web Server**, and click **Submit**.
The **Certificate Issued** page is displayed.
10. Click **Base 64 encoded**, and then click **Download certificate**.
11. When prompted, save the **certnew.cer** file.
12. Open the web console of the target device—iDRAC, CMC, or OpenManage Enterprise Modular (OME - Modular).
13. For iDRAC or CMC, click **Network** and click **SSL**.
For OME - Modular, click **Application Settings** → **Security** → **Certificates**.
14. To upload the certificate:
 - For iDRAC or CMC, select **Upload Server Certificate Based on Generated CSR** and click **Next**.
 - For OME - Modular, click **Upload** and click **Next**.
15. Click **Browse**, select the **certnew.cer** file you saved in step 11, and then click **Apply**.
16. Install the RootCA signed certificate (**newcert.cer**) as **Trusted Root Certificate Authorities** in the OpenManage Essentials management server:



NOTE: Ensure that the certificate file you want to install is a Base64 encoded certificate file issued by root CA.

- a. Right-click the **certnew.cer** file, and click **Install Certificate**.
The **Certificate Import Wizard** is displayed.
- b. Select **Local Machine** as the store location, and then click **Next**.
- c. Select **Place all certificates in the following store** and click **Browse**.
The **Select Certificate Store** dialog box is displayed.
- d. Select **Trusted Root Certification Authorities**, and click **OK**.
- e. Click **Next**.
- f. Click **Finish**.
The **Security Warning** dialog box is displayed.

g. Click **Yes**.

17. Close the web browser and open the web console of the target device in a new browser window.
18. Discover and inventory the WS-Man target(s), in OpenManage Essentials using the **newcert.cer** RootCA signed certificate file.


Discovering a chassis and its components by using Guided Wizard

When you discover a chassis using the **Chassis (CMC) Discovery — All Components** device type filter within the **Guided Wizard**, OpenManage Essentials automatically discovers the components in the chassis (blade servers and IOA switches). To discover the chassis and its components, you must provide the hostname or IP address and the WS-Man credentials of the chassis.


By default, the blade servers (iDRACs) in the chassis are discovered using the WS-Man credentials you provide for the chassis. If the credentials of the chassis and the iDRACs are not the same, you can provide an alternate WS-Man credentials for discovering the iDRACs.

 **NOTE:** If required, you can use the Guided Wizard to only discover the chassis.

 **NOTE:** Automatic discovery of the blade servers in a chassis is supported only for Dell's 11th or later generation of PowerEdge servers (iDRAC 6 or later).

 **NOTE:** For discovering a PowerEdge M1000e chassis and its components, ensure that CMC firmware version 5.0 or later is installed. If the firmware installed is prior to version 5.0, you must discover the chassis and its components individually using the Standard Wizard.

 **NOTE:** Automatic discovery of IOA switches is supported only if chassis firmware version 5.1 or later is installed on PowerEdge M1000e and chassis firmware version 1.3 or later is installed on PowerEdge FX2/FX2s.

 **NOTE:** To discover MX7000 chassis, you must provide the REST credentials. In a Multi-Chassis Management (MCM) group, provide the REST parameters of lead MX7000 chassis.

 **NOTE:** During the discovery of MX7000 chassis, if Secure Mode is not selected under REST Configuration Options then OpenManage Essentials ignores the following certificate errors:

- Common name errors
- Untrusted certificate authority errors
- Revocation errors

However, other certificate errors are not ignored by OpenManage Essentials.

To discover a chassis and its components by using Guided Wizard:

1. Click **Manage** → **Discovery and Inventory**.
The **Discovery and Inventory Portal** wizard is displayed.
2. Under **Common Tasks**, click **Add Discovery Range**.
The **Discovery Range Configuration** page of the **Discovery Devices** wizard is displayed.
3. Select the **Save as Group** option and enter a name for the group.


 **NOTE:** When discovering a chassis by using the guided wizard, you must save the discovery range as a group.

4. Enter the hostname or IP address of the chassis and click **Add**.
In a Multi-Chassis Management (MCM) group, provide the hostname or IP address of lead MX7000 chassis.
5. Click **Next**.
The **Device Type Filtering** page is displayed.
6. Select **Chassis (CMC) Discovery - All Components** and click **Next**.

 **NOTE:** To discover the MX7000 chassis, you must select **MX Chassis Discovery - All Components**.

The **ICMP Configuration** page is displayed.

7. If required, change the timeout and retries values based on your preference.
8. Click **Next**.
If you select **MX Chassis Discovery - All Components**, the **REST Configuration** page is displayed.

9. Select **Enable REST discovery** and enter the MX7000 chassis credentials.
 10. If required, change the timeout, retries and port values based on your preference, and then click **Next**.
The **WS-Man Configuration** page is displayed.
 11. Select **Enable WS-Man discovery** and enter the chassis credentials.
 12. If required, change the timeout, retries, and port values based on your preference, and then click **Next**.
 13. If you want to disable auto discovery of the chassis components or if you want to enter alternate credentials for discovering the iDRACs, click **Alternate WS-Man Configuration for iDRACs**.
 - To disable the auto discovery of iDRACs and switches, clear the **Auto discover iDRACs and switches in the CMC** option.
 - To provide alternate credentials for discovering the iDRACs, clear the **Use same credentials of CMC for discovering iDRACs** option, and enter the iDRAC username and password.
-  **NOTE:** If you have selected **MX Chassis Discovery - All Components only** in the **Device Type Filtering** page, enter the **WS-Man credentials to discover the chassis components**.
14. Click **Next**.
The **Summary** page is displayed.
 15. Review the protocol configurations and click **Finish**.
A job is initiated to discover the chassis and its components (iDRACs and IOA switches).

Excluding ranges

Configure exclude ranges to prevent servers from being discovered or rediscovered, or limit the number of devices displayed in the device tree.

To exclude a range from discovery task:

1. From OpenManage Essentials, select **Manage** → **Discovery and Inventory** → **Common Tasks** → **Add Exclude Range**.
2. In **Exclude Range Configuration**, provide IP address/range, discovery range name or host name, and click **Add**.
3. Click **Finish**.

Related links

[Discovery and Inventory Portal](#)
[Last Discovery and Inventory](#)
[Discovered Versus Inventoried Devices](#)
[Task Status](#)

Viewing configured discovery and inventory ranges


From OpenManage Essentials, click **Manage** → **Discovery and Inventory** → **Discovery Ranges** → **All Ranges**.

Related links

[Discovery and Inventory Portal](#)
[Last Discovery and Inventory](#)
[Discovered Versus Inventoried Devices](#)
[Task Status](#)

Scheduling discovery

1. Click **Manage** → **Discovery and Inventory** → **Common Tasks** → **Discovery Schedule**.
2. In **Discovery Schedule Settings**:
 - Select the desired schedule parameters.
 - (Optional) You may adjust the task speed slider for faster task execution; however, more system resources are consumed if the speed is increased.
 - Discover all instrumented devices.

 **NOTE: It is recommended not to schedule the discovery task at the same time as the Database Maintenance Execution Schedule, as the console is less responsive during database maintenance.**


Related links

[Discovery and Inventory Portal](#)
[Last Discovery and Inventory](#)
[Discovered Versus Inventoried Devices](#)
[Task Status](#)

Discovery Speed Slider

This control, also known as the discovery throttle, controls how fast discovery occurs and how much network and system resources are consumed for discovery by controlling the:

- Number of discovery threads that are allowed to run at any point of time.
- Delay in between the communicating devices during a network ping sweep, in milliseconds.

 **NOTE: Each tick on the throttle control equals 10% and the range is from 10% to 100%. By default, in OpenManage Essentials, the discovery throttle is set at 60%. After an upgrade from IT Assistant, the throttle control remains at its previously set value.**

Multithreading

OpenManage Essentials improves upon the optimized parallel threading implementation in the Network Monitoring Service introduced in IT Assistant.

As the discovery process is I/O intensive, you can optimize the process by making it a parallel operation, where threads running in parallel (known as multi-threading) send requests and handle responses to several devices simultaneously.

The more threads that run in parallel, each communicating to a different device, the faster is the discovery; barring overall high network congestion or latency. The discovery process, by default, allows a maximum of 32 threads to run in parallel (or concurrently) at any one time for discovery.

To control the number of parallel threads executing, move the discovery throttle control either left or right. When set at the maximum, 32 parallel threads are allowed to run. If the throttle is at 50%, only 16 threads are allowed to run at any one time.

As the discovery service is optimized for parallel threading operations, the system can utilize more system resources even at the same throttle setting. It is recommended that you monitor the system resources so that a satisfactory trade-off is made between discovery speed versus system resources available for OpenManage Essentials. Lowering or increasing the throttle depends on the system it is running on and the available resources. Note that the discovery service may take up to several minutes to adjust to a new throttle setting.

 **NOTE: For minimal discovery times on medium to large size networks (several hundred to several thousand devices), it is recommended that you install OpenManage Essentials services on a multi-processor system.**

Scheduling inventory

1. Click **Manage** → **Discovery and Inventory** → **Common Tasks** → **Inventory Schedule**.
2. In **Inventory Polling Configuration Settings**, perform the following:
 - Select **Enable Inventory**.
 - Select the desired schedule parameters.
 - (Optional) You may adjust the **Inventory Polling Speed** slider for faster task execution; however, more system resources are consumed.

 **NOTE: It is recommended not to schedule the inventory task at the same time as the Database Maintenance Execution Schedule, as the console is less responsive during database maintenance.**

Related links

[Discovery and Inventory Portal](#)
[Last Discovery and Inventory](#)
[Discovered Versus Inventoried Devices](#)
[Task Status](#)

Configuring status polling frequency

You can configure OpenManage Essentials to check the health status of all discovered devices that have a means of health instrumentation such as OpenManage Server Administrator. The status can be scheduled at a given interval using Status Polling so that health status is always current.

To configure status polling:

1. Click **Manage** → **Discovery and Inventory** → **Common Tasks** → **Status Schedule**.
2. In **Status Polling Schedule Settings**, select **Enable Status Polling** and provide the polling parameters including time and performance.
3. Click **OK**.

 **NOTE: It is recommended not to schedule status polling at the same time as the Database Maintenance Execution Schedule, as the console is less responsive during database maintenance.**

Related links

[Discovery and Inventory Portal](#)
[Last Discovery and Inventory](#)
[Discovered Versus Inventoried Devices](#)
[Task Status](#)

Task pop-up notifications

The task pop-up notification is displayed in the bottom-right corner of the OpenManage Essentials console when a task is completed. The information displayed in the task pop-up notification varies based on the number of completed tasks.

 **NOTE: The task pop-up notification is displayed only for tasks that create a Task Execution History.**

If only one task is completed, the following information is displayed:

- Status of the task — Indicates if the task was successful or unsuccessful.
- Task name as a link that you can click to view the Task Execution Details (if available).
- A link to open the portal related to the task.
- A link to access the task pop-up notification settings where you can disable task pop-up notifications.

If more than one alert is received, the following information is displayed:

- Number of tasks that are completed.
- Task names as links that you can click to view the Task Execution Details (if available).

 **NOTE: The task name link is displayed only for the first three tasks.**

- **Go to Alert Console** — To access the Alerts portal.
- **Disable** — To access the task pop-up notification settings.

By default, the alert pop-up notification is enabled. You can configure OpenManage Essentials to disable alert pop-up notifications or set the time interval between each alert pop-up notification.

 **NOTE: The Alert Pop-up Notification Settings is user-specific. The settings you have configured is not applicable to other users.**

Configuring task pop-up notifications

1. Click **Settings** → **Task Notification Settings**.
The **Task Notification Settings** page is displayed.
2. Under **Task Popup Notification Settings**, select or clear **Enable Task Popup Notifications** to enable or disable task pop-up notifications.
3. In the **seconds between popup notifications** box, select the time interval between each pop-up notification.
4. Click **Apply**.

Enabling or disabling task pop-up notifications



NOTE: To quickly disable alert pop-up notifications, click the **Disable** link displayed in the task pop-up notification. When the **Disable Task Popup Notifications** prompt is displayed, click **Yes**.

To enable or disable task pop-up notifications:

1. Click **Settings** → **Task Notification Settings**.
The **Task Notification Settings** page is displayed.
2. In **Task Popup Notification Settings**:
 - Select the **Enable Alert Popup Notifications** option to enable task pop-up notifications.
 - Clear the **Enable Alert Popup Notifications** option to disable task pop-up notifications.
3. Click **Apply**.

Discovery And Inventory — Reference

From the **Discovery and Inventory** portal page, you can:

- View graphical reports on devices and servers discovered and inventoried.
- Manage discovery ranges for devices and servers.
- Configure discovery, inventory, and status polling for devices and servers.

Discovery and Inventory Portal Page Options

- Discovery Portal
- Common Tasks
 - Add Discovery Range
 - Add Exclude Range
 - Discovery Schedule
 - Inventory Schedule
 - Status Schedule
- Discovery Ranges
- Exclude Ranges

Discovery and Inventory Portal

The Discovery and Inventory Portal provides information about the:

- Last discovery and inventory details
- Discovered versus inventoried devices
- Task status

Related links

[Creating a discovery and inventory task](#)
[Viewing configured discovery and inventory ranges](#)
[Excluding ranges](#)
[Scheduling discovery](#)
[Scheduling inventory](#)
[Configuring status polling frequency](#)
[Last Discovery and Inventory](#)
[Discovered Versus Inventoried Devices](#)
[Task Status](#)

Last Discovery and Inventory

Table 16. Last Discovery and Inventory

Field	Description
Last Discovery Details	
Discovery Last Run at	Displays the time and date information for the last run discovery.

Field	Description
Discovery Range	Displays the IP Address range or host name.
Devices Discovered	Displays information on number of devices discovered.
Last Inventory Details	
Inventory Last Run at	Displays the time and date information for the last run inventory.
Inventory Range	Displays the IP Address range or host name.
Devices Inventoried	Displays information on number of devices inventoried.

Related links

[Creating a discovery and inventory task](#)
[Viewing configured discovery and inventory ranges](#)
[Excluding ranges](#)
[Scheduling discovery](#)
[Scheduling inventory](#)
[Configuring status polling frequency](#)
[Discovery and Inventory Portal](#)

Discovered Versus Inventoried Devices

The graph displays the number of devices and servers discovered or inventoried. You can use this report to ascertain the discovered devices and servers that are unclassified. For more information on the filter options for the summary information, see [Viewing Device Summary](#).

Click any section of the graph to view the **Device Summary** for the selected region. In the device summary, double-click a row to view the details (inventory view for that device). Alternatively, right-click and select details for the inventory view or right-click and select alerts for the alerts specific to that device.

Table 17. Discovered Versus Inventoried Devices

Field	Description
Filter by	Select to filter the search results using the following options: <ul style="list-style-type: none"> • All • Ranges — Select to filter based on the selected range.

Related links

[Creating a discovery and inventory task](#)
[Viewing configured discovery and inventory ranges](#)
[Excluding ranges](#)
[Scheduling discovery](#)
[Scheduling inventory](#)
[Configuring status polling frequency](#)
[Discovery and Inventory Portal](#)

Task Status

The grid provides a list of currently executing and previously run tasks and their status. The **Task Status** grid on this page shows the status of just discovery, inventory, and tasks. However, the main portal shows all types of task statuses.

Related links

- [Creating a discovery and inventory task](#)
- [Viewing configured discovery and inventory ranges](#)
- [Excluding ranges](#)
- [Scheduling discovery](#)
- [Scheduling inventory](#)
- [Configuring status polling frequency](#)
- [Discovery and Inventory Portal](#)

Viewing Device Summary

1. In **OpenManage Essentials**, click **Manage** → **Discovery and Inventory** → **Discovery Portal** → **Discovery Portal**.
2. In **Discovered vs. Inventoried Devices** graphical report, click the bar representing the discovered or inventoried device to open the **Device Summary** page that displays the selected graph details.
3. (Optional) Click the funnel icon to filter the summary information.
The filter options are displayed. See [Viewing Device Summary Filter Options](#).
4. (Optional) Click **Filter** to view the filtered summary information.
5. (Optional) Click **Clear Filter** to remove the filtered summary information.
6. Right-click a device summary and select from the available options. See [Device Status](#).

Viewing Device Summary Filter Options

Table 18. Viewing Device Summary Filter Options

Field	Description
Select All	Select to filter per line item.
Select options, devices, or servers.	Select to filter based on options, devices, or servers.
Filter options	<p>Create filter with these options:</p> <ul style="list-style-type: none">• Is equal to— Select to create the <i>same as</i> logic.• Is not equal to — Select to create the <i>different from</i> logic.• Is Less than— Select to find a value that is less than the value you provide.• Is less than or equal to— Select to find a value that is less than or equal to the value you provide.• Is greater than or equal to— Select to find a value that is greater than or equal to the value you provide.• Is greater than— Select to find a value that is greater than the value you provide. <p>Health Status options:</p> <ul style="list-style-type: none">• Unknown• Normal• Warning• Critical <p>Connection Status options:</p> <ul style="list-style-type: none">• On• Off

Add Discovery Range


1. Click **Manage** → **Discovery and Inventory** → **Common Tasks**.
2. Click **Add Discovery Range**. For more information, see [Creating a Discovery and Inventory Task](#).
3. Provide information for the appropriate protocols for discovery, inventory, or for both:
 - Discovery Range Configuration
 - Device Type Filtering
 - ICMP Configuration
 - SNMP Configuration
 - WMI Configuration
 - Storage Configuration
 - REST Configuration
 - WS-Man Configuration
 - SSH Configuration
 - IPMI Configuration
 - Discovery Range Action
 - Summary



Discovery Configuration

A discovery range is a network segment registered in OpenManage Essentials for the purpose of discovering devices. OpenManage Essentials attempts to discover devices on all registered discovery ranges that are enabled. A discovery range includes subnet, a range of IP addresses on a subnet, an individual IP address, or an individual host name. Specify the IP address, IP address range, or host name for the discovery process. For more information, see [Discovery Configuration Options](#).

Discovery Configuration Options

Table 19. Discovery Configuration Options

Field	Description
Save as Group	Select this option to save the discovery range as a group.
Group Name	Specifies the group name for the discovery range.
IP address / range	<p>Specifies the IP address or IP address range.</p> <p>The following are examples of valid discovery range type address specifications (* is the wildcard character, meaning all possible addresses in the specified range):</p> <ul style="list-style-type: none">• 193.109.112.*• 193.104.20-40.*• 192.168.*.*• 192.168.2-51.3-91• 193.109.112.45-99• System IP address—193.109.112.99 <p> NOTE: Click Add to add multiple ranges of IP addresses. IPV6 addresses are not supported.</p>
Discovery Range Name	Specifies the discovery range name for the IP address/range.
Host name	Specifies the host name, for example, mynode.mycompany.com .

Field	Description
	<p>Click Add to add multiple host names.</p> <p> NOTE: You can add multiple host names by separating them using commas.</p> <p> NOTE: Invalid characters in the host name are not checked. If the host name you provide contains invalid characters, the name is accepted. However, the device is not found during the discovery cycle.</p>
Subnet mask	<p>Specifies the subnet mask for the IP address range. The subnet mask is used to determine the broadcast addresses for the subnet(s) part of the range. The OpenManage Essentials Network Monitoring Service does not use the broadcast address when discovering devices in an IP address range. The following are examples of valid subnet mask specifications:</p> <ul style="list-style-type: none"> • 255.255.255.0 (The default subnet mask for a Class C network.) • 255.255.0.0 (The default subnet mask for a Class B network.) • 255.255.242.0 (A custom subnet mask specification.) <p>By default, the subnet mask is set to 255.255.255.0.</p>
Import	<p>Select this option to import host names and IP addresses from a file that is in CSV format. However, you can import only 500 line items per task. You can import different discovery ranges with different subnet masks. For example, 192.168.10.10, 255.255.255.128, 10.10.1.1, 255.255.0.0, and 172.16.21.1, 255.255.128.0.</p> <p>You can use an Active Directory export file in a .CSV format as input. You can also create a .CSV file in a spreadsheet editor using the header <i>Name</i> and filling in system IP addresses or host names in the rows below the header (one per cell). Save the file in a .CSV format and use it as the input with the import feature. If there are any invalid entries in the file, a message is displayed when the data is imported by OpenManage Essentials. For an example of a CSV file, see Specifying IPs, Ranges, or Host Names.</p>

Device Type Filtering

The **Device Type Filtering** options are displayed in the **Discover Devices** wizard, if **Guided Wizard** is selected in [Discovery Settings](#). This window enables you to select device types for discovery. After the device types are selected, the required protocols for discovering and managing the selected device types are added to the **Discover Devices** wizard. For example, if you select **ESXi Host**, **SNMP Configuration** and **WS-Man Configuration** options are added to the wizard. The following table describes the fields displayed in the **Device Type Filtering** window.


 **NOTE: The device range that was discovered in the earlier version of OpenManage Essentials may have discovered both chassis and iDRAC using WS-Man protocol. In OpenManage Essentials version 2.5, if Discover the selected Device Types only option is enabled in Discovery settings, then only the specific device selected in the guided wizard will be discovered and other devices are classified as unknown devices. For example: Selecting iDRAC device type with WS-Man protocol will discover only iDRAC devices using WS-Man protocol.**


Table 20. Device Type Filtering

Field	Description
Device Type	Displays the device types that you can select to discover and manage.
Required Protocol	Displays the protocols that are required to discover and manage the selected device types.

ICMP Configuration

ICMP is used to by discovery engine to determine whether or not any device has a specified IP address. The discovery engine sends out a request and waits until the 'timeout' period to receive a reply. If a device is busy doing other things, it may not reply to an ICMP request as quickly as it would under low-load conditions. If no device has been assigned to the IP address being tested by the discovery engine, there will be no response at all. If no reply is received within the 'timeout' period, the discovery engine will repeat the request up to 'Retries' times (waiting, each time, for the 'timeout' period to expire). See [ICMP Configuration Options](#) to configure the ICMP parameters.

 **NOTE: ICMP ping is optional in OpenManage Essentials version 2.5. ICMP Configuration is displayed based on the selection of Skip ICMP ping during discovery under Settings → Discovery Settings → Skip ICMP ping during discovery.**

For more information, click the help () icon.

ICMP Configuration Options

Table 21. ICMP Configuration Options

Field	Description
Timeout (milliseconds)	Specifies the maximum number of milliseconds the discovery engine waits for a reply after issuing an ICMP request. The default timeout period is 1000 milliseconds. A higher value allows more time to receive responses from busy devices, but also means more wait time if there is no device with a specified IP address.
Retries (attempts)	Specifies the maximum number of additional times that the discovery engine will send an ICMP request if the first request times out. A device may have been too busy to respond to an earlier ICMP request, but may be able to respond to a subsequent request. If there is no device with the IP address being used, retries will also timeout, so the retry count should be a small number. The default value is 1.


SNMP Configuration

SNMP provides an interface to manage devices on the network such as servers, storage, switches, and so on. The SNMP agent on the device allows OpenManage Essentials to query the health and inventory data of the device. See [SNMP Configuration Options](#) to discover and inventory servers, storage devices, and other network devices.

For more information, click the help icon  .

SNMP Configuration Options

Table 22. SNMP Configuration Options

Field	Description
Enable SNMP discovery	Enables or disables the SNMP protocol for discovery range (subnet).
Enable SNMP V1/V2c	
Get community	Specifies the community name for SNMP get calls from the OpenManage Essentials user interface. The Get Community is a read-only password that SNMP agents installed on managed devices use for authentication. The Get Community allows OpenManage Essentials to browse and retrieve SNMP data. This field is case-sensitive. OpenManage Essentials uses the first successful community name to communicate with the device. You can enter multiple SNMP community strings separated with commas. For more information, see Configuring SNMP Services on Windows .
Set community	<p>Specifies the community name for SNMP set calls from the OpenManage Essentials UI. The Set community is a read-write password that SNMP agents installed on managed devices use for authentication. The Set community allows OpenManage Essentials to perform tasks that require the SNMP protocol, such as shutting down a system.</p> <p>This field is case-sensitive. You can enter multiple SNMP community strings separated with commas. OpenManage Essentials uses the first successful community name to communicate with the device.</p> <p> NOTE: In addition to the Set community name, an instrumentation password is required to perform an SNMP task on a device.</p>
Enable SNMP V3	
Authentication Protocol	Specifies the authentication protocol for the discovery of the devices. The supported authentication protocols are MD5 and SHA1. The device must be configured using the same authentication protocol for the discovery to be successful. If the authentication protocol is selected to be none, then the encryption option is also disabled.
User Name	Specifies the username configured on the device.
Authentication Password	Specifies the authentication password.
Encryption Protocol	Specifies the encryption protocol for the discovery of the devices and is optional. The supported encryption protocols are AES and DES. The device must be configured using the same encryption protocol for the discovery to be successful.
Encryption Password	Specifies the authentication password.
Generic Settings	
Timeout (seconds)	Specifies the maximum number of seconds the discovery engine waits after issuing a get or set call before it considers the call failed. A valid range is 1–15 seconds. The default is 4 seconds.
Retries (attempts)	Specifies the maximum number of additional times the discovery engine reissues a get or set call after the first call times out. The discovery engine reissues the call until it is successful, or all retry

Field	Description
	attempts have timed out. A valid range is 1–10 retries. The default is 2.

WMI Configuration

Use the WMI protocol for collection data about discovery, inventory, and health information of Windows servers. This protocol provides less information about devices than SNMP but is useful if SNMP is disabled on the network. See [WMI Configuration Options](#) to configure WMI parameters for Windows servers only.

WMI Configuration Options

Table 23. WMI Configuration Options

Field	Description
Enable WMI discovery	Select to enable WMI discovery.
Domain \ User name	Provide the domain and user name.
Password	Provide the password.

Storage Configuration

Enabling discovery of PowerVault MD or Dell EMC arrays allows OpenManage Essentials to collect data about inventory and health information about the arrays. See [Storage Configuration Options](#) to discover PowerVault MD arrays or Dell EMC devices.

Storage Configuration Options

Table 24. Storage Configuration Options

Field	Description
Enable PowerVault MD array discovery	Select to discover PowerVault MD array. This discovery configuration does not require credentials.
Enable Dell EMC array discovery	Select to discover Dell EMC array.
Dell EMC user name	Provide the user name.
Dell EMC password	Provide the password.
Dell EMC port	Increment or decrement the port number. Enter a TCP/IP port number ranging 1 to 65535. Default value is 443.

WS-Man Configuration

Use the WS-Man protocol to discover and collect data about inventory and health status for the iDRAC, ESXi based servers, PowerEdge VRTX, PowerEdge FX devices, and VxFlex Ready Nodes. For more information, see [WS-Man Configuration Options](#).

 **NOTE:** You can only discover and inventory servers with iDRAC6 version 1.3 and later. Discovery and inventory of servers is not supported for iDRAC6 version 1.25 and earlier.

WS-Man Configuration Options

Table 25. WS-Man Configuration Options

Field	Description
Enable WS-Man Discovery	Select to discover PowerEdge FX, PowerEdge VRTX, iDRAC6, iDRAC7, iDRAC8, and ESXi installed devices.
User ID	Provide authenticated user ID.
Password	Provide password.
Timeout (seconds)	Enter a number to indicate the time that the discovery engine must wait for before timing out after requesting for a WS-Man connection. The valid range is from 1 to 360 seconds. The default time is 15 seconds.
Retries (attempts)	By default, four attempts. If the first request times out, indicates the maximum number of repeated attempts that the discovery engine will make by resending a WS-Man connection request to a device. Valid range is 1–10 attempts.
Port	Provide the port information. The default port number is 623.
Secure Mode	Select to securely discover devices and components.
Skip Common name check	Select to skip common name check.
Trusted Site	Select if the devices you are discovering is a trusted device.
Certificate file	Click Browse to navigate to the file location.

Alternate WS-Man Configuration for iDRACs (Guided Wizard only)

Table 26. Alternate WS-Man Configuration for iDRACs (Guided Wizard only)

Field	Description
Auto discover iDRACs and switches in the CMC	<ul style="list-style-type: none">• Select to automatically discover the iDRACs and switches in the CMC while discovering the chassis.• Clear to disable the automatic discovery of the iDRACs and switches in the CMC. Only the chassis is discovered.
Use same credentials of CMC for discovering iDRACs	<ul style="list-style-type: none">• Select to discover the iDRACs in the CMC using the credentials you provided for the CMC.• Clear to provide different credentials for discovering the iDRACs in the chassis.

REST configuration

Use the REST protocol to discover and collect data about inventory and health status of the MX7000 chassis. In an MCM group, enter the REST credentials of the lead MX7000 chassis during discovery. After the discovery, inventory and health status of lead chassis, member chassis, compute sleds, and storage in the MCM group are gathered. The compute sleds in the MX7000 chassis are discovered using the WS-Man protocol. See [WS-Man Configuration](#).

REST configuration options

 **NOTE:** During the discovery of MX7000 chassis, if **Secure Mode** is not selected under REST Configuration Options then OpenManage Essentials ignores the following certificate errors:

- Common name errors
- Untrusted certificate authority errors
- Revocation errors

However, other certificate errors are not ignored by OpenManage Essentials.

Table 27. REST configuration Options

Field	Description
Enable REST Discovery	Select to discover the MX7000 chassis.
User ID	Enter an authenticated user ID.
Password	Enter the chassis password.
Timeout (seconds)	Enter a number to indicate the time that the discovery engine must wait for before timing out after requesting for a REST connection. The valid range is from 1 to 360 seconds. The default time is 15 seconds.
Retries (attempts)	By default, four attempts. If the first request times out, indicates the maximum number of repeated attempts that the discovery engine makes by resending a REST connection request to a device. Valid range is 1–10 attempts.
Port	Enter the port information. The default port number is 443.
Secure Mode	Select to securely discover devices and components.

SSH Configuration

Use the SSH protocol to discover and inventory servers running Linux. See [SSH Configuration Options](#) to configure the SSH configuration parameters.

SSH Configuration Options

Table 28. SSH Configuration Options




Field	Description
Enable SSH discovery	Enables or disables the SSH protocol by discovery range.
User name	Enter the username.
Password	Enter the password.
Port	Specifies the port information. The default port number is 22.
Retries (attempts)	By default, three attempts. If the first request times out, indicates the maximum number of repeated attempts that the discovery engine makes by resending an SSH connection request to a device. Valid range is 1–10 attempts.
Timeout (seconds)	Enter a number to indicate the time that the discovery engine must wait for before timing out after requesting for an SSH connection. The valid range is from 1 to 360 seconds. The default time is 3 seconds.

IPMI Configuration

Use the IPMI protocol for out of band discovery of RACs, DRACs, and iDRACs. This option is for Lifecycle controller enabled discovery and inventory. Ensure that the IP address of the DRAC and iDRAC is selected. See [IPMI Configuration Options](#) to configure the IPMI version 2.0 parameters. This configuration is required for discovery.

IPMI Configuration Options

Table 29. IPMI Configuration Options

Field	Description
Enable IPMI Discovery	Enables or disables the IPMI protocol by discovery range.
User name	Enter the Baseboard Management Controller (BMC) or DRAC user name.  NOTE: The default user name is root. It is recommended that you change it for security.
Password	Enter the BMC or DRAC password.  NOTE: The default password is calvin. It is recommended that you change it for security.
KG Key	Enter the KG key value. DRAC also supports IPMI KG key value. Each BMC or DRAC is configured to require an access key in addition to user credentials.  NOTE: The KG key is a public key that is used to generate an encryption key for use between the firmware and the application. The KG key value is an even number of hexadecimal characters.
Timeout (seconds)	Enter a number to indicate the time that the discovery engine waits after sending an IPMI request. The valid range is from 1 to 60 seconds. The default time is 5 seconds.
Retries (attempts)	By default, one attempt. If the first call times out, indicates the maximum number of repeated attempts that the discovery engine makes by resending an IPMI request to a device. Valid range is 0–10 attempts.

 **NOTE: The retries and time-out parameters are used for both the Remote Management Control Protocol (RMCP) ping and the IPMI connection.**

Discovery Range Action

Select these options to discover or inventory devices, components, and servers.

Table 30. Discovery Range Action

Field	Description
Do not perform discovery or inventory	Select this option to set up a schedule to perform discovery and inventory (at a later time).
Perform only discovery	Select this option to perform discovery.
Perform both discovery and inventory	Select this option to perform both discovery and inventory.

Summary

View the configuration selections. To change configurations, click **Back**.


Add Exclude Range

From OpenManage Essentials, select **Manage** → **Discovery and Inventory** → **Common Tasks** → **Add Exclude Range**. Register new ranges to exclude from discovery or to remove a previously set exclude range.

You can also right-click **Exclude Ranges** and select **Add Exclude Range**.

Add Exclude Range Options

Table 31. Add Exclude Range Options

Field	Description
IP address / range	Register a device to exclude from the discovery process by specifying the IP address or IP address range of the device. The following are examples of valid discovery range type address specifications (* is the wildcard character, which includes all possible addresses in the specified range): <ul style="list-style-type: none">Exclude range — 193.109.112.*193.104.20-40.*192.168.*.*192.168.2-51.3-91Exclude range — 193.109.112.45-99System IP address — 193.109.112.99
Name	Add the exclude range name for the IP address / range.
Host name	Register to exclude from the discovery process by specifying the host name of the device, for example, mynode.mycompany.com .  NOTE: OpenManage Essentials does not check for invalid characters in the host name. If the host name you specify contains invalid characters, the name is accepted. However, the device with that name is not found during the discovery cycle.

Discovery Schedule

You can configure OpenManage Essentials to discover devices and display them in the **Device** tree.

- Enable device discovery.
- Initiate device discovery.
- Set the discovery speed.
- Specify how devices are discovered.
- For failed discovery attempts, use the Troubleshooting Tool.

Related link

[Discovery Schedule Settings](#)

Viewing Discovery Configuration

To view discovery configuration, click **Manage** → **Discovery and Inventory** → **Discovery Schedule**.

Discovery Schedule Settings

Configure OpenManage Essentials to discover new devices on a network. The settings apply to all discovery ranges. OpenManage Essentials records all agents, IP addresses, and the health of the devices.

Table 32. Discovery Schedule Settings

Field	Description
Enable Discovery	Select to schedule device discovery.
Configure Global Device Discovery interval	<p>Set the frequency of discovery in weekly or daily intervals.</p> <ul style="list-style-type: none">• Every Week On — Specify the day or days to schedule discovery and the time for the discovery to begin.• Every <n> Days <n> Hours interval — Specify the intervals between discovery cycles. The maximum discovery interval is 365 days and 23 hours.
Discovery Speed	Specify the amount of resources (system and network) available for accelerating the discovery speed. The faster the speed, more resources are required to perform discovery, but less time is required.
Discover	<p>Specify how the devices are discovered.</p> <ul style="list-style-type: none">• All Devices — Select to discover all devices that respond to an Internet Control Message Protocol (ICMP) ping. ICMP ping is optional in OpenManage Essentials version 2.4 and later. To skip ICMP ping during discovery, click Settings → Discovery Settings → Skip ICMP ping during discovery. If selected, ICMP ping is skipped during discovery and inventory of the devices.• Instrumented Devices — Select to discover only devices that have instrumentation (such as OpenManage Server Administrator, OpenManage Array Manager, and Networking Ethernet switches) for Simple Network Management Protocol (SNMP), Windows management Instrumentation WMI), Intelligent Platform Management Interface (IPMI) management, or WS-Management (WS-Man). See agents supported for more information about systems management instrumentation agents.
Name Resolution	<p>Specify how the device names are resolved. If you are managing a cluster, use the NetBIOS name resolution to discern each independent system. If you are not managing a cluster, a DNS name resolution is recommended.</p> <ul style="list-style-type: none">• DNS — Select to resolve names using the Domain Naming Service.• NetBIOS — Select to resolve names using system names.

Related link

[Discovery Schedule](#)

Inventory Schedule


Use **Inventory Polling** to specify the default inventory settings for OpenManage Essentials. OpenManage Essentials collects inventory information such as software and firmware versions, as well as device-related information about memory, processor, power supply, Peripheral Component Interconnect (PCI) cards, and embedded devices, and storage.

Related link

[Inventory Schedule Settings](#)

Inventory Schedule Settings

Table 33. Inventory Schedule Settings

Field	Description
Enable Inventory	Select to schedule inventory.
Configure Global Inventory Polling Interval	<p>Set the frequency of the inventory in weekly or daily intervals.</p> <p> NOTE: OpenManage Essentials performs inventory only on devices that have already been discovered.</p> <ul style="list-style-type: none">• Every Week On — Specify the day or days of the week that you want to schedule the inventory and the time that you want it to begin.• Every <n> Days <n> Hours interval — Specify the intervals between inventory cycles. The maximum discovery interval is 365 days and 23 hours.
Inventory Polling Speed	<p>Set the amount of resources available for accelerating the inventory poll speed. The faster you set the inventory poll speed, the more resources are required, but less time is required to perform the inventory.</p> <p>After changing the speed, OpenManage Essentials may take several minutes to adjust to the new speed.</p>

Related link

[Inventory Schedule](#)

Status Schedule

Use this window to specify the default status polling settings for OpenManage Essentials. Status polling performs a health and power check for all discovered devices. For example, this poll determines if discovered devices are healthy or powered down.


Related link

[Status Polling Schedule Settings](#)

Status Polling Schedule Settings

Table 34. Status Polling Schedule Settings

Field	Description
Enable OnDemand Poll	Select to query the global status of the device when an alert is received from the device.







Field	Description
	 NOTE: If a large number of alerts are received, multiple OnDemand polls are queued up and it may affect the system performance. In this scenario, it is recommended to turn off OnDemand poll and enable the regular status poll interval to retrieve the health status of managed devices. If OnDemand poll is disabled, the device status only updates on the normal status poll.
Enable Status Polling	Select to schedule device status polling.
Device Status Interval	Set frequency of the device status poll in intervals of days, hours, and minutes. The status polling does not begin until the previous polling has completed. Days — Specify the number of days between device status polling. Hours — Specify the number of hours between device status polling cycles. Minutes — Specify the number of minutes between device status polling cycles. The maximum discovery interval is 365 days, 23 hours, and 59 minutes.
Status Polling Speed	Set the amount of resources available for accelerating the device status polling speed. The faster you set the status speed, the more resources are required, but less time is required to perform the status polling.

Related link

[Status Schedule](#)

Discovery Ranges

The **Discovery Ranges** section displays all the IP address or IP address ranges that you have configured for discovery. The icon displayed beside the discovery range varies based on the type of wizard used for discovery.

- If you configure a discovery range using the **Standard Wizard** the  icon is displayed.
- If you configure a discovery range using the **Guided Wizard**, the  icon is displayed.
 - If you discover a chassis using the **Guided Wizard**, the chassis range group displays the  icon. The members of the chassis range group that are dynamically discovered displays the  icon. If the chassis range group is disabled, the  icon is displayed. If the members of the range group are disabled, the  icon is displayed.

 **NOTE: In an MCM group, the discovery ranges of the lead MX7000 chassis and the member compute sleds are displayed.**

You can also right-click a discovery range to see the options available on the discovery range. For information on the right-click options, see [Managing Include Ranges](#).

Exclude Ranges

The **Exclude Ranges** section displays the IP address or IP address ranges that you have configured to exclude from the discovery process.

Managing devices

OpenManage Essentials lists devices based on their types. For example, PowerEdge servers are listed under the device type **Servers**. OpenManage Essentials contains a defined list of device types. The devices you discover and inventory are included under these device types. Unclassified devices are listed under the device type **Unknown**. You can create device groups with combinations of the defined device types. However, you cannot create a new device types.

In the **Devices** page, you can:

- View devices types that are discovered on the network.
- View the inventory information for the devices.
- View all alerts that were generated for a device.
- View all noncompliant devices associated with a catalog baseline in a device group.
- View all noncompliant devices associated with a configuration baseline in a device group.
- View hardware logs for a device.
- Create device groups and include devices to that group based on your grouping preference. For example, you can create a group and include all devices present at a geographical location.
- Display and manage PowerEdge VRTX and FX2/FX2s devices using **Map View**.

Related links

[Viewing devices](#)

[Viewing device inventory](#)

[Viewing alerts summary](#)

[Viewing System Event Logs](#)

[Searching for Devices](#)

[Creating a New Group](#)

[Adding Devices to a New Group](#)

[Adding Devices to an Existing Group](#)

[Hiding a Group](#)

[Deleting a Group](#)

[Creating a Custom URL](#)

[Using Map View](#)

Viewing devices

You can view a device that is discovered. For more information on discovering and inventorying a device, see [Discovering and Inventorying Devices](#).

To view devices, click **Manage** → **Devices**.

Related link


[Managing devices](#)


Device Summary Page


On the Device Summary page, expand the device types to view the devices. The following device types are displayed:


- **Citrix XenServers**
- **Clients**
- **Clusters**


- HA Clusters
 - NAS Clusters
 - Hyper-Converged Infrastructure
 - VxRail
 - XC Series
 - KVM
 - Microsoft Virtualization Servers
 - Virtual machines
 - Modular systems
 - PowerEdge Chassis
 - PowerEdge FX2
 - PowerEdge M1000e
 - PowerEdge MX7000

 **NOTE:** In a Multi-Chassis Management (MCM) group, only the lead MX7000 chassis is displayed.

 - PowerEdge VRTX
-  **NOTE:** The blade servers (iDRACs) in the chassis are discovered using the WS-Man credentials you provide for the chassis and are listed under the RAC group. If both DRAC and iDRAC, and their corresponding server are discovered, they are correlated into a single device. This device is then displayed under both RAC and Servers groups.
- Network Devices
 - Networking Switches
 - Fibre Channel Switches
 - Network Appliances
- OEM Devices
- OOB Unclassified Devices
 - IPMI Unclassified Devices
- Power Devices
 - PDU
 - UPS
- PowerEdge C Servers
- Printers
- RAC

 **NOTE:** If a DRAC or iDRAC is discovered, it is displayed under the RAC group and not under the Servers group. If both DRAC and iDRAC, and their corresponding server are discovered, they are correlated into a single device. The device is then displayed under both RAC and Servers group.


 **NOTE:** If the RAC on a PowerEdge C server is discovered using IPMI, it is displayed under OOB Unclassified devices.
- Repurpose and Bare Metal

 **NOTE:** Devices in the Repurpose and Bare Metal group are displayed as targets for device configuration deployment. You must explicitly add devices to this group for deploying a device configuration. On bare metal deployments, you can remove the devices from the Repurpose and Bare Metal group after the deployment is complete. For more information, see [Server Deployment and Re-provisioning](#).
- Servers
- Storage Devices
 - Dell Compellent Arrays
 - Dell EqualLogic Groups
 - Dell NAS Appliances

- Dell EMC Arrays
- PowerVault MD Arrays
- Tape Devices
- Unknown
- VMware ESX servers
 - Virtual machines
- VxFlex Ready Nodes







 **NOTE:** If you delete the VxFlex Ready Nodes custom group then you need to recreate this group with the respective query. See [Creating a New Group](#).

Use the refresh button to update the device tree with the current data. To update the device tree, right-click **All Devices** and select **Refresh**.

 **NOTE:** The device tree auto-updates when changes are made. Some changes to the tree may appear after a brief delay depending on the performance of the managed servers because the information propagates from the SQL database to the user interface.

Nodes and symbols description

Table 35. Nodes and Symbols Description


Node Symbol	Description
 Figure 15. Critical device icon	Denotes that a device is critical and requires attention. This information is rolled up to the parent device type. For example if a server is in critical state and requires attention the same symbol is assigned to the parent device type. Among server states, critical state is given the highest priority. That is, in a group, if different devices are in different states, and if one device is in critical state, then the state of the parent device type is set to critical.
 Figure 16. Device not discovered icon	Denotes that a device of this type is not discovered on the network or classified in the device tree.
 Figure 17. Deviation from expected behavior icon	Denotes that there is a deviation from the expected behavior, but the device is still manageable.
 Figure 18. Device working as expected icon	Denotes that the device is working as expected.
 Figure 19. Unknown device icon	Denotes either the device type is unknown and it is classified as an unknown device or that the health status cannot be determined, because the device does not have proper instrumentation or the proper protocol was not used to discover the device.
 Figure 20. Connection Lost	Denotes that the device is not reachable.

Device details

The device details, depending on the device type, might contain the following information:

Table 36. Device details

Device details	
<ul style="list-style-type: none"> • Device Summary • OS Information • Data Sources • NIC Information • Virtual Machine Host Product Information • RAC Device Information • Processor Information • Memory Device Information • Firmware Information • Power Supply Information • Embedded Device Information • Device Card Information • Controller Information • Controller Battery Information • Enclosure Slot Information • Physical Disk Information • Virtual Disk Information • Contact Information • Appliance Node Information • Switch Device Information • EqualLogic Volume Information • Device Properties • Storage Group Information • iDRAC Information • Storage Information 	<ul style="list-style-type: none"> • Tape Drive Information and Tape Library Information • Physical Battery Information • Fluid Cache Information • Fluid Cache Pool Information • Fluid Cache Disk • Software Inventory Information • Trusted Platform Module Information • Slot Information • Virtual Flash Information • FRU Information • Printer Cover Table • Printer Marker Supplies Information • Printer Input Tray Information • Printer Output Tray Information • Acquisition Information • Depreciation Information • Lease Information • Maintenance Information • Service Contract Information • Extended Warranty Information • Ownership Information • Outsource Information • Maser Information • Chassis Group Information • I/O Module Information

 **NOTE:** The warranty information (including expired and renewed) displayed in OpenManage Essentials for a particular Service Tag, may not match with the warranty record displayed at Dell.com/support. The service level code and model name of a warranty record displayed at Dell.com/support may not exactly match with the OpenManage Essentials warranty report.

 **NOTE:** The Data Sources table in the device inventory displays the Dell Command | Monitor (previously OMCI) agent name as System Administrator.

 **NOTE:** Hardware inventory can be retrieved from iDRAC6/7 and ESXi if OpenManage Server Administrator VIB is installed using WS-Man protocol.

 **NOTE:** The Data Sources table in the device inventory displays information about the iDRAC Service Module only if:

- iDRAC is discovered.
- iDRAC is discovered and the server is discovered using WMI or SSH protocol.

Viewing device inventory

To view inventory, click **Manage** → **Devices**, expand the device type and click the device.


Related link

[Managing devices](#)

Viewing alerts summary

You can view all the alerts that are generated for a device. To view the alert summary:

1. Click **Manage** → **Devices**.
2. Expand the device type, and click the device.
3. On the details page, select **Alerts**.

 **NOTE:** In an MCM group, alerts are displayed if all the member chassis, compute sleds, storage, and IOMs are included in the alert policy that is configured for the lead MX7000 chassis. If alert policies are configured individually, alerts of the member MX7000 chassis and compute sleds are not displayed in the alert summary. To view the alerts of the member chassis, see [Viewing alert logs](#).

Related link

[Managing devices](#)

Viewing noncompliant devices associated with a catalog baseline

1. Click **Manage** → **Devices**.
2. To view all noncompliant devices associated with a catalog baseline, click **All Devices**.
All the noncompliant devices are listed in the **Non-Compliant Firmware & Drivers** tab.
3. To view noncompliant devices of a custom device group, expand **All Devices**, and click the required device group.
On the **Non-Compliant Firmware & Drivers** tab, all noncompliant devices of the selected group are listed. The catalog baseline that is associated with the custom device group is also listed.

For more information about applying system updates, see [Applying system updates by using the Non-Compliant Systems tab](#).

Viewing noncompliant devices associated with a configuration baseline

1. Click **Manage** → **Devices**.
2. To view all noncompliant devices, click **All Devices**.
All the noncompliant devices are listed in the **Non-Compliant Configurations** tab.
3. To view noncompliant devices in a device group, expand **All Devices**, and click the required device group.
On the **Non-Compliant Configurations** tab, all noncompliant devices of the selected group are listed. The configuration baseline that is associated with the individual device is also listed.

To remediate the noncompliant devices, see [Remediating noncompliant devices](#).

Viewing System Event Logs

1. Click **Manage** → **Devices**.
2. Expand the device type and select **Hardware Logs**.

Related link

[Managing devices](#)

Searching for Devices

Right-click **All Devices** at the top of the device tree and click **Search Devices**. You can also search for devices using logical arguments and save the queries for later.

For example, to create a query to search for a server in critical state with an IP address containing values 10.35, and the power status as Power Up:

1. Click **Manage** → **Device Search**, then select **Create New Query**, in the adjacent text field enter a query name.
2. From the first line after **Where**, select **Device Type, Is**, and then **Server**.
3. In the next line select the check box, then select **AND, Device Health, Is**, and then select **Critical**.
4. In the next line select the check box, then select **AND, IP Address, Contains**, and then in the adjacent field enter **10.35**.
5. In the next line select the check box, then select **AND, Power Status, Is**, and then select **Power Up**.
6. Click **Save Query**.


 **NOTE:** You can click **Run Query** to run the query immediately.

To run an existing query, select the query from the drop-down list and click **Run Query**. You can filter the results and export it to an HTML, TXT, or CSV file.

Related link

[Managing devices](#)

Creating a New Group

1. Click **Manage** → **Devices**.
2. Right-click **All Devices** and select **New Group**.
3. Enter the name and description for the group and click **Next**.
4. In **Device Selection**, select any of the following:
 - **Select a query** to create a dynamic group. Click **New** to create a new query or select an existing query from the drop-down list.
 **NOTE:** To create a query for VxFlex Ready nodes:
 1. Include ScaleIO as the device model.
 2. In the next line select the check box, then select **OR**, and then include VxFlex as the device model.
 - **Select the device(s) /group(s) from the tree below** to create a static group.
5. Click **Next**.
6. Review the summary and click **Finish**.

You can right-click devices in the **Details** tab and add them either to a new group or an existing group. You can also create a new group from either the Home or Reports portal. Click **Filter by** and click **Add New Group** to launch the **New Group** wizard. To know whether a group is static or dynamic, place the cursor on the group. For example, if you place the cursor on **Servers**, the group type is displayed as **Servers (Dynamic | System)**.

Related link

[Managing devices](#)

Adding Devices to a New Group

1. Click **Manage** → **Devices**.
2. Right-click the device(s) and select **Add to New Group**.
3. In **Group Configuration**, enter the name and description. Click **Next**.
4. In **Device Selection**, the selected devices are displayed. If required, add or remove additional devices. Click **Next**.
5. Review the summary and click **Finish**.

Related link

[Managing devices](#)

Adding Devices to an Existing Group

1. Click **Manage** → **Devices**.
2. Right-click the device(s) and select **Add to Existing Group**.



NOTE: If you are manually adding a device to a dynamic group, a message is displayed on the screen. Manually adding a device to a dynamic group changes the group from dynamic to static, thereby removing the original dynamic query. If you want the group to remain dynamic, modify the query defining the group. Click **Ok** to continue or **Cancel** to stop the procedure.

3. Click **Ok**.

Related link

[Managing devices](#)

Hiding a Group

To hide a group, right-click the group and select **Hide**.

After a group is hidden, it is not displayed in any of the device group controls in the console. The devices in the hidden groups are not displayed in the reports and charts on the Home and Reports portals. Alerts for devices in hidden groups are also not displayed in the alerts portal.

If a parent group (along with child groups) is hidden, the child groups are also hidden in the device tree. However, the child groups are still present in the database and are displayed in other instances in the console.

Related link

[Managing devices](#)

Deleting a Group

1. Right-click the group and select **Delete**.
2. In the **Delete** screen, click **Yes**.



NOTE: Deleting a parent group, removes the group from the device tree. The child groups and devices listed under the parent group are also removed from the device tree. However, the child groups and devices still remain in the database and appear in other instances in the console.

Related link

[Managing devices](#)

Associating a catalog baseline to custom device groups

To associate a catalog baseline to VxFlex Ready Nodes, you must download the latest catalog and packages by right-clicking the discovered Ready Node and clicking **Application Launch** → **VxFlex Ready Node Series Support**.

1. Click **Manage** → **Devices**.
2. Right-click a custom device group and select **Associate Catalog Baseline**.
3. In **Associate Catalog Baseline**, do one of the following:
 - Select a catalog baseline from the list of catalog baselines.
 - Create a catalog baseline by importing a repository manager file.
4. Click **Finish**.
Custom device group is associated with the catalog baseline.
5. Click **Ok**.

In the **Non-Compliant Firmware & Drivers** tab, all noncompliant devices of the selected group are listed.

For more information about applying system updates, see [Applying system updates by using the Non-Compliant Systems tab](#).

Disassociating a catalog baseline from custom device groups


1. Click **Manage** → **Devices**.
2. Right-click a custom device group and select **De-associate Catalog Baseline**.
3. Click **Yes**.
Catalog baseline is disassociated.
4. Click **Ok**.
The compliance status of the custom device group is updated under the **Non-Compliant Firmware & Drivers** tab.


Single Sign-On


If iDRAC or CMC devices are configured for Single Sign-On and you are logged on to OpenManage Essentials as a domain user, you can use open the iDRAC or CMC console through the **Application Launch** option or the agent link. For information on configuring iDRAC or CMC for Single Sign-On, see the following:

- *Configuring CMC For Single Sign-On Or Smart Card Login* section in the *Dell Chassis Management Controller User's Guide* at dell.com/support/manuals.
- *Configuring iDRAC7 for Single Sign-On or Smart Card Login* section in the *Integrated Dell Remote Access Controller 7 User's Guide* at dell.com/support/manuals.
- *Integrating iDRAC7 With Microsoft Active Directory* white paper at DellTechCenter.com.
- *iDRAC6 Integrated Dell Remote Access Controller 6 Security* white paper at DellTechCenter.com.

Creating a Custom URL

 **NOTE:** Custom URL cannot be assigned to parent device groups that create a child sub group in the device tree at the time of discovery. Examples of parent device groups are: HA Clusters, Microsoft Virtualization Servers, PowerEdge M1000e, PowerEdge VRTX, or VMware ESX Servers. To assign a custom URL to a device in these parent device groups, add the device to a custom device group, and then assign a custom URL.

1. Click **Settings** → **Custom URL Settings**.
2. Click the  icon.
The **Custom URL Launch** screen is displayed.
3. Type the name, URL, description, and select the device group from the drop-down list.

 **NOTE:** You can click **Test URL** to verify if the URL specified is active.

4. Click **Ok**.
The custom URL is created.

Related links

[Managing devices](#)
[Custom URL Settings](#)

Launching the Custom URL

1. Click **Manage** → **Devices** and select the device from the tree.
2. Right-click the device and select **Application Launch**.
3. Click the URL name to access the site.



Related link

[Custom URL Settings](#)

Configuring Warranty Email Notifications

You can configure OpenManage Essentials to send a warranty notification of your devices at periodic intervals through email. For information about the options you can configure, see [Warranty Notification Settings](#).

To configure **Warranty Email Notifications**:

1. Click **Settings** → **Warranty Notification Settings**.
The **Warranty Notification Settings** page is displayed.
2. Under **Warranty Email Notifications**, select **Enable Warranty Email Notifications**.
3. In the **To** field, type the email addresses of the recipients.
 **NOTE: Multiple email addresses must be separated by using a semicolon.**
4. In the **From** field, type the email address from which the warranty notification email is to be sent.
 **NOTE: Only one email address must be provided in the From field.**
5. To set the criteria for the devices to be included in the warranty notification email, in the **All Devices with x Days or less of warranty** field, select the number of days.
6. To set the frequency at which you want to receive the warranty notification email, in the **Send email every x Days** field, select the number of days.
7. To include devices with expired warranty or no warranty information in the warranty notification email, select **Include Expired Warranties**.
8. In the **Next Email will Send On** field, select the date and time at which you want to receive the next warranty notification e-mail.
9. If you want to configure the SMTP email server, click **Email Settings**.
The **Email Settings** page is displayed. For more information about **Email Settings**, see [Email Settings](#).
10. Click **Apply**.

OpenManage Essentials sends warranty notification emails based on your configuration. The warranty notification email provides a list of devices and appropriate links that you can click to renew the warranty of the devices.

Related link

[Warranty Notification Settings](#)

Configuring Warranty Scoreboard Notifications

You can configure OpenManage Essentials to display a warranty scoreboard notification icon in the heading banner. For information about the options you can configure, see [Warranty Notification Settings](#).

To configure **Warranty Scoreboard Notifications**:

1. Click **Settings** → **Warranty Notification Settings**.
The **Warranty Notification Settings** page is displayed.
2. Under **Warranty Scoreboard Notifications**, select **Enable Warranty Scoreboard Notifications**.
3. To set the criteria for the devices to be included in the warranty notification scoreboard, in the **All Devices with x Days or less of warranty** field, select the number of days.
4. To include devices with expired warranty or no warranty information in the warranty notifications scoreboard, select **Include Expired Warranties**.
5. Click **Apply**.

If any device meets the set criteria, the OpenManage Essentials heading banner displays the warranty scoreboard notification icon including the number of devices.

Related links

[Using the Warranty Scoreboard Notification Icon](#)

[Device Warranty Report](#)

[Warranty Notification Settings](#)

Configuring Warranty Pop-Up Notifications

You can configure OpenManage Essentials to display warranty pop-up notifications based on the warranty status of the devices. For information about the options you can configure, see [Warranty Notification Settings](#).

To configure warranty pop-up notifications:

1. Click **Settings** → **Warranty Notification Settings**.
The **Warranty Notification Settings** page is displayed.
2. In **Warranty Popup Notification Settings**:
 - Select the **Enable Warranty Popup Notifications** option to enable warranty pop-up notifications.
 - Clear the **Enable Warranty Popup Notifications** option to disable warranty pop-up notifications.
3. Click **Apply**.

Configuring Warranty Update Settings

You can configure OpenManage Essentials to check the warranty information of the discovered devices on the support site. For information about the options you can configure, see [Warranty Notification Settings](#)


To configure warranty update settings:


1. Click **Settings** → **Warranty Notification Settings**.
The **Warranty Notification Settings** page is displayed.
2. Under **Warranty Update Settings**, select **Enable Warranty Updates**.
3. In the **Update warranty every** field, select the number of days to set the frequency at which the warranty updates are checked.
4. In the **Next warranty update will be on** field, select the date and time at which you want to check the next warranty updates.
5. Click **Apply**.

 **NOTE:** By default, the **Warranty Update Settings** is disabled. You can view the warranty information in the **Device Warranty Report**.

Using Map View

 **NOTE:** For information about using the features available in Map View, see [Map View \(Home\) Portal](#).

 **NOTE:** The map displayed in Map View should be considered *as is* from the map service provider. OpenManage Essentials does not have any control over the accuracy of the map or address information.

 **NOTE:** An Internet connection is required to perform some of the map functions such as zoom, address search, and so on. If you are not connected to the Internet, the following message is displayed on the map: **Warning – Unable to connect to the Internet!**.


 **NOTE:** A valid map provider (MapQuest or Bing) key is required for the Map View functionality. To enter the map provider key, see [Configuring Map Settings](#).

The **Map View** feature allows the display and management of PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license on an interactive geographic map. PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license are represented as pins on the map. The health and connectivity status can be viewed for all PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license at a glance.

You can access **Map View** from the **Home Portal** or **Manage** → **Devices** portal page.

The **Overlays** menu at the top-right of the map allows you to overlay the health and connectivity status of the device on the pin. The **Actions** menu at the top-right of the map allows you to perform various functions on the map. The following is the list of available actions:

Table 37. Using Map View

Action	Description
Show All Map Locations	Displays all map locations.
Go to Home View	Displays the home view, if saved earlier.
Save Current View as Home View	Saves the current view as the home view.
Add Licensed Device	Allows adding PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license.
Import Licensed Devices	Allows importing PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license.
Remove All Map Locations	Allows removing all map locations.
Export	Allows exporting all map locations to a .csv file.
Settings	Opens the Map Settings dialog box.
Edit Location Details	Opens the Edit Location Details dialog box, that displays the device name, address, and contact information.
Remove Location	Allows removal of the selected device from the map.
Zoom to Street Level	Allows zooming to the street level on the currently selected device location.
 NOTE: This option is displayed only when a device is selected on the map.	

 **NOTE:** The **Edit Location Details**, **Remove Location**, and **Zoom to Street Level** options in the **Actions** menu are device-specific. These options must be used after selecting a device on the map.

The **Search for address** box at the top-left of the map allows you to search for addresses.

The navigation toolbar displayed at the bottom of the map enables you to:

- Zoom in and out of the map
- Move the map up, down, right, or left
- Select the map provider type



Figure 21. Navigation Toolbar

The zoom level of the map can be identified by the scale that is displayed at the bottom-right of the map.

Related links

[Devices — Reference](#)
[Map View—Home Portal](#)
[Map View Interface—Home Portal](#)
[General Navigation and Zooming](#)
[Home View](#)
[Tool Tip](#)
[Search Pin](#)
[Map Providers](#)
[Map View Interface—Devices Tab](#)
[Configuring Map Settings](#)
[Selecting a Device on Map View](#)
[Health and Connection Status](#)
[Multiple Devices at the Same Location](#)
[Setting a Home View](#)
[Viewing All Map Locations](#)
[Adding a Device to the Map](#)
[Moving a Device Location Using the Edit Location Details Option](#)
[Importing Licensed Devices](#)
[Using the Map View Search Bar](#)
[Adding a Device Using the Search Pin](#)
[Moving a Device Location Using the Search Pin](#)
[Removing All Map Locations](#)
[Editing a Map Location](#)
[Removing a Map Location](#)
[Exporting All Device Locations](#)
[Managing devices](#)

Map Providers






You can select between MapQuest and Bing map providers using the  icon in the navigation toolbar. By default, the map is displayed using the MapQuest provider. The following table provides information about the supported map providers.

Table 38. Map Providers

MapQuest	Bing
Requires a valid MapQuest key (license) that must be purchased based on the number of transactions per month. To view the available transaction plans, go to developer.mapquest.com/plans/ . After getting a valid MapQuest key, you must provide the key in the Map Settings dialog box.	Requires a valid Bing maps key that must be purchased. To get a valid Bing maps key, go to microsoft.com/maps/ .  NOTE: For instructions on getting a Bing maps key, see “Getting a Bing Maps Key” at microsoft.com. After getting a valid Bing maps key, you must provide the key in the Map Settings dialog box.
Internet connection is mandatory to render the online portion of the map and for the address lookup.	Internet connection is mandatory to access any zoom level and to use the search functionality.
If your system connects to the internet through a proxy server, the Proxy Settings configured in the OpenManage Essentials Settings → General Settings page is used.	If your system connects to the internet through a proxy server, the proxy settings configured in your web browser is used.
	Two types of maps are available: <ul style="list-style-type: none">• Roads map — A simple, fast loading map with minimal details.

MapQuest	Bing
	<ul style="list-style-type: none"> • Satellite map — Provides detailed satellite views of the world.

 **NOTE: The MapQuest and the Bing map providers require an internet connection at all times to render the map. If the system connects to the internet through a proxy server, the proxy settings configured in your web browser is used by the MapQuest and Bing providers.**

Related link

[Using Map View](#)

Configuring Map Settings

 **NOTE: Only OpenManage Essentials Administrators and Power Users are permitted to configure Map Settings.**

The **Map Settings** dialog box allows you to enable or disable the Internet connection status notification and to provide a valid Bing key required by the Bing map provider or MapQuest key required by the MapQuest map provider.

To configure the map settings:

1. Perform one of the following:
 - Click **Home** → **Map View**.
 - Click **Manage** → **Devices** → **Map View**.
2. On the **Map View**:
 - Right-click anywhere on the map, and then click **Settings**.
 - Move the mouse pointer over the **Actions** menu, and click **Settings**.

The **Map Settings** dialog box is displayed.

3. Select **Update map view on any device or device group selection** if you want the map to display only the pin or pins that correspond to the device or device group selected in the device tree.
4. Select **Show internet connection warning when unable to connect to the internet** if you want to display a warning on the map if an Internet connection is not available.
5. Select one of the following map providers:
 - **MapQuest**
 - **Bing**
6. In the **Key** field, type the appropriate map provider key.
7. Click **Apply**.

Related link


[Using Map View](#)

General Navigation and Zooming

To move the map, click and drag the map in the desired direction or use the navigation arrows in the Navigation toolbar.

You can zoom in or zoom out of the map using any of the following methods:

- Double-click a pin to zoom in to street level around that pin. You can also zoom in to street level by:
 - Right-clicking a pin, and then clicking **Zoom to Street Level**
 - Moving the mouse pointer over the **Actions** menu, and then clicking **Zoom to Street Level**
- If a pin is displayed at street level, double-click the pin to zoom out to the world-level view
- Double-click a location on the map to zoom-in one level at that location
- Move the mouse wheel up or down to quickly zoom out or in on the map

- Click the magnifying glass icon  in the navigation toolbar to display a slider that you can use to zoom in or zoom out of the map

 **NOTE: Zoom level and the visible portion of the Map View (home) portal are not synchronized with the Map View tab accessible through the Devices portal.**

Related link

[Using Map View](#)

Home View

If you have saved a particular region of the map as your home view, by default, the map displays the home view when you open the **Map View**. For instructions to set a region on the map as your home view, see [Setting a Home View](#).

Related link

[Using Map View](#)

Tool Tip

Moving the mouse pointer over the pin displays a tool tip that contains the following information:


- Device name
- Description
- Address
- Contact
- Model
- Service Tag
- Asset Tag
- Global status
- Connection status

Related link

[Using Map View](#)

Selecting a Device on Map View

To select a device on the map, click the appropriate pin. The corresponding device is highlighted in the device tree and all the other pins are hidden. When a device is selected in the device tree, it is also reflected on the map. If the **Modular Systems** or **PowerEdge VRTX** group is selected in the device tree, then all the pins placed for those groups are displayed on the map.

 **NOTE: Hiding a device group in the device tree does not hide the corresponding pins on the map. For example, hiding the Modular Systems group in the device tree does not hide pins on the map that represent devices in the Modular Systems group.**

 **NOTE: Clicking a pin on the Map View (home) portal opens the Devices portal that displays details about the device.**





Related link

[Using Map View](#)

Health and Connection Status



The health and connection status of a device can also be displayed on the map. To overlay the pin with the health or connection status of the device, move the mouse pointer over the **Overlays** menu at the top-right of the map, and click **Health** or **Connectivity**. The health or connection status is indicated by the color and the icon displayed within the pin. The following table provides information about the health status and pin overlay:

Table 39. Health Status

Pin Color	Icon	Health Status
Red		Critical
Yellow		Warning
Green		Normal
Gray		Unknown

The following table provides information about the connection status and pin overlay:

Table 40. Connection Status

Pin Color	Icon	Connection Status
Blue		On
Grey		Off

Related link

[Using Map View](#)

Multiple Devices at the Same Location

It is possible for two or more licensed devices to be placed at an identical location. These devices are displayed as a multi-pin group on the map. If the devices are in a very close proximity on the map and the map is zoomed out, the pins are displayed together as a multi-pin group. To view the count and the name of the devices in a multi-pin group, move the mouse pointer over the multi-pin group. Double-click or right-click a multi-pin group and then select **Details**, to open the **Devices at this location** window that lists the devices available at the location. On the **Devices at this location** window, you can:

- Double-click a device to display only that device on the map.
- Right-click a device to view standard options for the devices, such as **Refresh Inventory**, **Application Launch**, and so on, and other map-specific options such as **Edit Location Details**, and so on.

 **NOTE:** Only licensed devices can be placed on the map. Device groups cannot be placed on the map.

Related link

[Using Map View](#)

Setting a Home View

If you typically manage devices in a certain geographic region, you can set that region as your home view. Each OpenManage Essentials user can save a different view of the map as their home view. By default, the home view is displayed when you open **Map View** or when you select the **Go to Home View** option.

1. Perform one of the following:
 - Click **Home** → **Map View**.
 - Click **Manage** → **Devices** → **Map View**.
2. On the **Map View**, navigate and zoom until the current view is as desired.
3. Perform one of the following:
 - Right-click on the map, and then click **Save Current View as Home View**.
 - Move the mouse pointer over the **Actions** menu, and then click **Save Current View as Home View**.

Related link

[Using Map View](#)

Viewing All Map Locations

If a single device is selected, only that device is displayed on the map. To view all map locations that have been placed on the **Map View**:

- Right-click the map, and click **Show All Map Locations**.
- Move the mouser pointer over the **Actions** menu, and click **Show All Map Locations**.

Related link

[Using Map View](#)

Adding a Device to the Map

 **NOTE:** Only PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license that are not already placed on the map can be added to the map.


 **NOTE:** Only OpenManage Essentials Administrators and Power Users are permitted to add a device to the map.

To add a device on the map:

1. Perform one of the following:
 - Click **Home** → **Map View**.
 - Click **Manage** → **Devices** → **Map View**.
2. On the **Map View**:
 - Right-click the map, and click **Add Licensed Device**.
 - Move the mouser pointer over the **Actions** menu, and click **Add Licensed Device**.

The **Device Location Details** dialog box is displayed.

3. From the **Devices** list, select the device you want to add.
4. If required, in the **Description** field, type an appropriate description for the device.
5. If you want to add the device at a location different from where you right-clicked on the map, in the **Address** field, type the address of the location. For example, Chicago.

 **NOTE:** Using the **Address** field to add a device on the map requires an Internet lookup through the map provider to resolve the provided address. The device is added to the most appropriate location available from the Internet lookup. If the map provider is not able to resolve the address, a message is displayed.

6. If required, in the **Contact** field, type the contact information.
7. Click **Save**.

Related links

[Using Map View](#)

[Adding a Device Using the Search Pin](#)

Moving a Device Location Using the Edit Location Details Option

 **NOTE:** Only OpenManage Essentials Administrators and Power Users are permitted to edit a map location.

1. Perform one of the following:
 - Click **Home** → **Map View**.
 - Click **Manage** → **Devices** → **Map View**.
2. Right-click a pin on the map, and select **Edit Location Details**.
The **Device Location Details** dialog box is displayed.

3. In the **Address** field, type the location name or airport code. For example, New York.



NOTE: Using the **Address** field to move a device location requires an Internet lookup through the map provider to resolve the provided address. The device is moved to the most appropriate location available from the Internet lookup. If the map provider is not able to resolve the address, a message is displayed, and the device remains at the current location.

4. Click **Save**.

If the map provider is able to resolve the address or airport code, the pin is moved to the specified location on the map.

Related links

[Using Map View](#)

[Moving a Device Location Using the Search Pin](#)

Importing Licensed Devices



NOTE: Only PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license that are not already placed on the map can be imported to the map.



NOTE: Only OpenManage Essentials Administrators and Power Users are permitted to import licensed devices.



NOTE: You can only import a maximum of up to 500 devices at a time.

You can bulk import licensed devices on the map through a .csv file. An **Export Template** function is available, which creates a .csv file that is already populated with the names of the licensed PowerEdge VRTX and PowerEdge FX2/FX2s devices that are currently discovered.

To import licensed devices:

1. Perform one of the following:
 - Click **Home** → **Map View**.
 - Click **Manage** → **Devices** → **Map View**.
2. On the **Map View**, do one of the following:
 - Right-click the map, and click **Import Licensed Devices**.
 - Move the mouse pointer over the **Actions** menu, and click **Import Licensed Devices**.

The **Import Licensed Devices** dialog box is displayed.

3. Click **Export Template** to download a .csv template that you can use for importing licensed PowerEdge VRTX devices.



NOTE: For more information about the template, see [Template for Importing Devices](#).

The **Save As** dialog box is displayed.

4. Browse to the location where you want to save the .csv file, type an appropriate file name, and click **Save**.
5. Open the .csv file, and perform one of the following:
 - In the **Latitude** and **Longitude** columns, type the latitude and longitude coordinates for each device.
 - In the **Address** column, type the address for each device. For example, 1 dell way, round rock, TX.



NOTE: Before you import devices using the address, ensure that the system is connected to the Internet. If the system connects to the Internet through a proxy server, verify if the proxy settings are configured in the **Settings** → **General Settings** page. Also, the Internet search provider may reject the address search request if you are attempting to import too many devices at a time. If this occurs, wait for some time and try importing again.

6. Click **Import**.
The **Open** dialog box is displayed.
7. Select the location where the updated .csv file is located, and click **Open**.
The **Import Summary** dialog box is displayed.
8. Click **Ok**.



NOTE: Any errors that may occur during the import process are displayed in Logs → UI Logs.

Related links

[Using Map View](#)

[Template for Importing Devices](#)

Template for Importing Devices

The template for importing PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license is a **.csv** file that you can use to provide details about devices that you want to import to the map. The following are the fields available in the template:

Table 41. Template for Importing Devices

Field	Description
Name	The name of the PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license. This field is already populated with the currently discovered PowerEdge VRTX devices with an Enterprise license that are not already placed on the map.
Latitude	The latitude coordinate of the device location.
Longitude	The longitude coordinate of the device location.
Address	The address of the device location. If both latitude and longitude coordinates are specified, the address need not be specified.
Description (Optional)	Any information that you want to include about the device.
Contact (Optional)	Any contact information that you want to include for the device..

To import the PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license to the map, you must update the **.csv** file with one of the following:

- Latitude and Longitude
- Address

Related link

[Importing Licensed Devices](#)

Using the Map View Search Bar



NOTE: The map providers may not be able to resolve all addresses or airport codes correctly.

The search bar on **Map View** enables you to search for locations on the map using an address or airport code. To search for a location, type the location name or airport code (for example, New York or JFK) in the search bar, and either press <Enter> or click the arrow icon. If the map provider is able to resolve the address or airport code, a search pin is displayed at the specified location on the map.

Related link

[Using Map View](#)

Search Pin

The search pin is a larger pin that represents the search result on the map. The following are the characteristics of the search pin:

- At any instance, only one search pin can be located on the map. The search pin is displayed on the map at a location until you remove it or perform a new search. To remove the search pin, right-click the search pin and click **Remove**.
- Unlike the device pin, the search pin does not overlay any status.
- Double-clicking the search pin allows you to zoom in and zoom out of the location.
- Move the mouse pointer over the search pin to display a tool tip that includes the address of the location.
- You can add or move a licensed PowerEdge VRTX and PowerEdge FX2/FX2s devices at the search pin location.

Related link

[Using Map View](#)

Adding a Device Using the Search Pin

 **NOTE:** Only PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license that are not already placed on the map can be added to the map.

 **NOTE:** Only OpenManage Essentials Administrators and Power Users are permitted to add a device to the map.

1. Perform one of the following:
 - Click **Home** → **Map View**.
 - Click **Manage** → **Devices** → **Map View**.
2. Type the address or airport code (for example, New York or JFK) in the search bar, and either press <Enter> or click the arrow icon.
If the map provider is able to resolve the address or airport code, a search pin is displayed at the location on the map.
3. Right-click the search pin and click **Add Licensed Device Here**.
The **Device Location Details** dialog box is displayed.
4. From the **Devices** list, select the device you want to add.
5. Click **Save**.

Related links

[Using Map View](#)

[Adding a Device to the Map](#)

Moving a Device Location Using the Search Pin

 **NOTE:** Only OpenManage Essentials Administrators and Power Users are permitted to add a device to the map.

To move a device location:

1. Perform one of the following:
 - Click **Home** → **Map View**.
 - Click **Manage** → **Devices** → **Map View**.
2. Select the pin for a licensed PowerEdge VRTX or PowerEdge FX2/FX2s devices on the map.
3. Type the address or airport code (for example, New York or JFK) in the search bar, and either press <Enter> or click the arrow icon.
If the map provider is able to resolve the address or airport code, a search pin is displayed at the location on the map.
4. Right-click the search pin and click **Move Selected Device Here**.
5. On the **Move Device** confirmation dialog box, click **Yes**.
The selected device is moved to the location of the search pin.

Related links

[Using Map View](#)

[Moving a Device Location Using the Edit Location Details Option](#)

Removing All Map Locations

 **NOTE:** Only OpenManage Essentials Administrators and Power Users are permitted to remove all map locations.

To remove all map locations:

1. Perform one of the following:
 - Click **Home** → **Map View**.

- Click **Manage** → **Devices** → **Map View**.
2. On the **Map View**:
 - Right-click the map, and click **Remove All Map Locations**.
 - Move the mouser pointer over the **Actions** menu, and click **Remove All Map Locations**.

The **Remove All Map Items** dialog box is displayed prompting for your confirmation.

3. Click **Yes**.

Related link

[Using Map View](#)

Editing a Map Location

 **NOTE:** Only OpenManage Essentials Administrators and Power Users are permitted to edit a map location.

To edit a map location:

1. Right-click a pin on the map, and select **Edit Location Details**.
The **Device Location Details** dialog box is displayed.
2. In the **Description** field, edit the description as required.
3. If you want to move the device to a new location, in the **Address** field, type the location name.
4. In the **Contact** field, edit the contact information as required.
5. Click **Save**.

Related link

[Using Map View](#)

Removing a Map Location

 **NOTE:** Only OpenManage Essentials Administrators and Power Users are permitted to remove a map location.

To remove a location on the map:

1. Perform one of the following:
 - Click **Home** → **Map View**.
 - Click **Manage** → **Devices** → **Map View**.
2. On the **Map View**, right-click the location you want to remove and select **Remove Location**.
The **Delete Location** dialog box is displayed prompting for your confirmation.
3. Click **Yes**.

Related link

[Using Map View](#)

Exporting All Device Locations

Exporting all device locations allows you to save the information about the devices and their latitude and longitude coordinates as a **.csv** file. If the address is known for a pin, it is included in the **Description** field of the **.csv** file. Using this file, you can import the device locations at any time.

 **NOTE:** By default, the latitude and longitude coordinates of each device is saved to the **.csv** file, even if the latitude and longitude coordinates were not provided previously.

To export all device locations currently placed on the map:

1. On the **Map View**, move the mouse pointer over the **Actions** menu, and then click **Export**.

The **Save As** dialog box is displayed.

2. Browse to the location where you want to save the .csv file, type an appropriate file name, and click **Save**.

Related link

[Using Map View](#)

PowerEdge FX Chassis View

By default, the PowerEdge FX2 and FX2s chassis are classified in the device tree under **All Devices** → **Modular Systems** → **PowerEdge FX**. The compute sleds installed in the PowerEdge FX chassis, when discovered, are displayed under the appropriate PowerEdge FX device group in the device tree.

When a PowerEdge FX chassis is selected in the device tree, a graphical representation (**Chassis View**) of the front of the chassis is displayed in the device details page. The inventory information of the chassis is displayed under the **Chassis View**.

 **NOTE: The Chassis View is only displayed if the PowerEdge FX chassis is discovered using the WS-Man protocol, and at least one of the slots is occupied by a sled.**

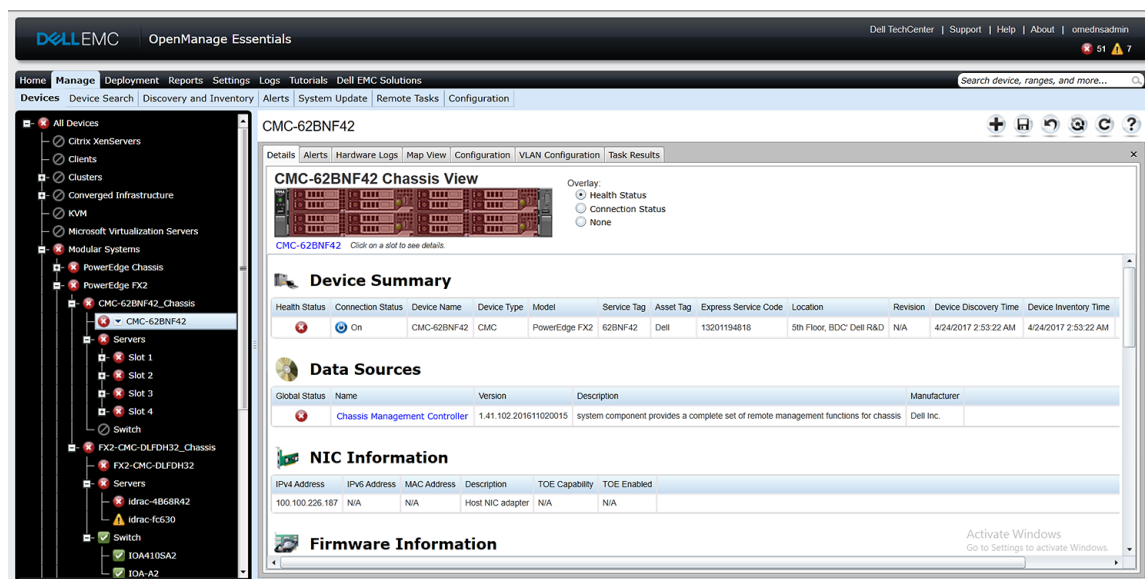


Figure 22. Chassis View

Tool Tip and Device Selection

Moving the mouser pointer over a slot on the chassis displays a yellow rectangular box around the slot and a tool tip.

 **NOTE: The tool tip is only displayed if the slot has a sled installed.**

The information displayed in the tool tip varies based on the discovery and inventory status of the sleds. If a sled that contains multiple compute nodes (For example, PowerEdge FM120x4) is discovered and inventoried, the tool tip displays the:

- Slot name
- Health status
- Connection status

If any other compute sled is discovered and inventoried and for storage sleds, the tool tip displays the:

- Slot name
- Sled model
- Service Tag
- Asset tag

- Health status
- Connection status

To select a slot, click the visual representation of the sled in the **Chassis View**. When a slot is selected, a yellow rectangular box is displayed around the sled.

- If a slot with a compute sled is selected, the sled inventory, if available, is displayed under the **Chassis View**.
- If slot with a sled that contains multiple compute nodes is selected, a summary of discovered devices (nodes) is displayed under the **Chassis View**. To view the inventory information of a node, double-click the node in the summary.
- If a slot with a storage sled is selected, the chassis inventory information is displayed under the **Chassis View**. The storage sled inventory information is displayed in the chassis inventory.

 **NOTE: Complete inventory information of a sled is displayed only if the chassis and sled are discovered using the appropriate protocol.**

 **NOTE: If a sled is selected in the device tree, the Chassis View is not displayed. To display the Chassis View, click the PowerEdge FX chassis in the device tree.**

Overlays


If a slot is occupied and the compute sled is discovered, by default, the health status of the compute sled is overlaid in the **Chassis View**. The following are the available overlay options and their descriptions.

Table 42. Overlays

Overlay Option	Overlay Color	Device Status
Health Status	Red	Warning
	Yellow	Critical
	Light gray	Unknown
Connection Status	Dark gray	Off (disconnected)
	No overlay	On (connected)
None	No overlay	Not applicable

 **NOTE: The health and connection status of a compute sled requires that the sled is discovered. If a sled is not discovered or the status of the sled is unknown, the health and connection status are displayed as normal.**

The health status of the sled that contains multiple compute nodes reflects the health status of the compute node with most critical severity. For example, if one compute node is in a **Warning** state and the remaining compute nodes are in a **Critical** state, the sled displays **Critical** status.

 **NOTE: The Chassis Management at Server Mode option of the PowerEdge FX chassis can be used to configure rack style management. If rack style management is disabled on a PowerEdge FX chassis, the health status roll-up of the chassis is not updated in OpenManage Essentials. Also, alerts generated from the PSU and fan are not received in OpenManage Essentials.**

Right-Click Actions

The right-click action on any compute sled that is discovered and available in the device tree is the same as when you right-click the sled in the device tree.

 **NOTE: Right-click actions are not available for sleds that contain multiple compute nodes and storage sleds.**

Navigation Trail

The navigation trail is displayed as a link under the **Chassis View** and indicates the currently selected device. You can click a device name in the navigation trail to go back to the chassis inventory.

Support For PowerEdge FX Chassis Sleds

The sleds that can be installed in the PowerEdge FX2 and PowerEdge FX2s chassis may vary. The following are the types of sleds and their support in OpenManage Essentials:

- Compute sleds — Require discovery and inventory for getting the inventory information and other functionality. Discovery and classification of these sleds can be performed using OMSA (in-band) or iDRAC (out-of-band).
- Storage sleds — These sleds are not discoverable and are not displayed in the device tree, device summary, or any typical locations for a device. The storage sled is displayed in the **Chassis View** and the storage sled inventory is displayed in the chassis inventory page.
- Sleds with multiple compute nodes — An example of this type of sled is the PowerEdge FM120x4 sled which contains four compute nodes. If the compute nodes of the sled are discovered, they are displayed in the device tree under: **All Devices** → **Modular Systems** → **PowerEdge FX** → **Chassis Group** → **Sled Group** → **Server Node**. Each compute node is displayed under the corresponding sled. The **Sled Group** name in the device tree can be edited if necessary.

 **NOTE: For in-band (without OMSA) discovery and monitoring of the PowerEdge FM120x4 sled, ensure that either the WMI or SSH protocol is enabled and setup.**

 **NOTE: The sleds installed in a PowerEdge FX chassis are sorted based on the device name and not on the slot number in the device tree.**


VLAN Configuration Management

The VLAN Configuration tab enables you to:

- View details of the blade server and IOA fabric interconnect such as the blade server NIC port, the associated IOA fabric port, and the VLAN IDs.

 **NOTE: Even if there is no information available for the IOAs, the fabric status is shown as data in grid and values such as Slot is empty and Firmware or Mode is not supported.**

- Assign VLAN IDs to the IOAs within the chassis.

 **NOTE: If an already discovered IOA or server is moved from one chassis to another, removed from a chassis, or swapped within the chassis, you must delete and rediscover the chassis, servers, and the corresponding IOAs. Otherwise, the VLAN configuration inventory may display duplicate or incorrect data.**

Requirements for VLAN Configuration Management

- VLAN configuration management is supported only for PowerEdge M1000e and PowerEdge FX2 or FX2s chassis.

 **NOTE: For VLAN configuration management on MX7000 chassis, see [Editing a device deployment template](#).**

- The chassis and its components (blade servers and IOAs) must be discovered in OpenManage Essentials using the Guided Wizard.
- The IOAs must be configured in Standalone, Virtual Link Trunk (VLT), or Programmable MUX (PMUX) operational mode.
- The minimum required firmware version is as follows:
 - PowerEdge M1000e—firmware version 6.1.
 - PowerEdge FX2 or FX2s—firmware version 2.1.
 - PowerEdge M and FN IOA
 - OpenManage Essentials version 2.5 supports 9.10.0.0, 9.10.0.1P10, 9.11.0.0, 9.11.2.0, 9.13.0.0, and 9.14.0.0.

 **NOTE: VLAN configuration management is not supported for the PowerEdge FM120x4 sleds. Only the server-chassis slot mapping is displayed in the VLAN Configuration tab for the PowerEdge FM120x4 sleds. The server name and NIC port details are not displayed in the VLAN Configuration tab for the PowerEdge FM120x4 sleds.**


Viewing the VLAN Configuration Inventory

To view the VLAN configuration inventory of a chassis:

1. Click **Manage** → **Devices**.
2. In the device tree, click **Modular Systems**.
3. Click **PowerEdge M1000e** or **PowerEdge FX2** and then click the chassis CMC node.
4. On the right pane, click the **VLAN Configuration** tab.

The VLAN configuration inventory is displayed.



NOTE: If you are accessing the VLAN Configuration tab for the first time, click the refresh icon  that is displayed at the middle of the VLAN Configuration tab to display the configuration inventory.



NOTE: The VLAN configuration inventory that is displayed may not be up-to-date. To view the latest VLAN



configuration inventory, click the refresh icon that is displayed at the top-right of the VLAN Configuration tab.



NOTE: VLAN configuration inventory is not displayed if the IOAs are not discovered or configured.

Even though the VLAN configuration inventory is not displayed, OpenManage Essentials displays the IOA Name and Model information if it is available. Otherwise a status message is displayed, indicating the reason for the non-availability of the inventory information.

The following table describes the status messages that may be displayed.

Table 43. Viewing the VLAN Configuration Inventory

Status	Description
Device not discovered	The IOA is not discovered in OpenManage Essentials.
Slot is empty	The chassis fabric slot is empty.
Firmware or Mode not supported	The operational mode or firmware version of the IOA is not supported.
Unable to retrieve data	OpenManage Essentials is unable to retrieve the VLAN configuration inventory from the IOA.
Unknown/Error	An error occurred or the status is unknown.
Model not supported	The IOA model is not supported.

Assigning VLAN IDs

Before you begin, ensure that you have IOA administrator rights.

To apply VLAN assignments:

1. On the **VLAN Configuration** tab, under **Chassis IOA**, type the VLAN IDs in the **Tagged VLANs** and **Untagged VLAN** columns for the appropriate ports.



NOTE: The valid range for VLAN IDs are 1 to 4094. Use a comma (,) to separate VLAN IDs and use a hyphen (-) to specify the ID range.

2. Click **Apply**.

The **VLAN Configuration** window displays the IOA ports that you modified.



NOTE: You can also modify the VLAN IDs in the VLAN Configuration window.

3. Type a unique name of the task.



NOTE: It is recommended that you enter a unique name for the task.

4. If required, select a schedule for the task.
5. Type the credentials of the IOA that have fabric administrator rights.
6. Click **Finish**.

The **VLAN Configuration** task is displayed in the **Task Results** tab. After the task is completed, OpenManage Essentials automatically inventories the VLAN configuration of the IOAs on the chassis.



NOTE: While applying VLAN assignments to multiple ports, the VLAN configuration task may fail. The Task Results tab displays the ports to which the VLAN assignments failed with a message stating that the task failed after multiple retries or the server closed the network connection unexpectedly. In such a scenario, you can retry the VLAN configuration after some time to the ports were not configured successfully.



NOTE: OpenManage Essentials uses the IOA CLI commands to configure the VLAN on the IOA. Configuring the VLAN on the IOA is a time consuming and resource-intensive operation that may affect the performance of the IOA. To balance the operations on the IOA, OpenManage Essentials runs the IOA CLI commands in a timely manner, ensuring that there is sufficient time to configure the VLAN on the IOA. If the IOA is already running several operations, the VLAN configuration task may either be prolonged or fail. If the VLAN configuration fails on some IOA ports, you can rerun the VLAN configuration task on the corresponding IOAs.

Resetting all VLAN IDs

Before you begin, ensure that you have fabric administrator rights.

After you make changes to VLAN IDs, if you want to revert all the changes:

1. Click **Reset All**.
2. When you are requested to confirm, click **Yes**.



NOTE: The changes you made to the VLAN IDs are affected only in the OpenManage Essentials user interface.

Setting the Default VLAN ID Values

Before you begin, ensure that you have fabric administrator rights.

If you want to set the default VLAN IDs:

1. Select the IOA fabric port that you want to set to the default VLAN ID.
2. Click **Set to default value**.
The tagged VLAN column displays **All VLANs** and the untagged VLAN column displays **1**.



NOTE: For tagged VLANs, the default value of All VLANs ranges from 2 to 4094. For untagged VLAN, the default value is 1.


3. Click **Apply**.
4. Type a unique name of the task.
5. If required, select a schedule for the task.
6. Type the credentials of the IOA that have fabric administrator rights.
7. Click **Finish**.

The **VLAN Configuration** task is created in the **Task Results** tab. After the task is completed, OpenManage Essentials automatically inventories the VLAN configuration of all IOAs in the chassis.

Dell NAS Appliance Support

The following table provides information about discovery and classification, availability of appliance node information, and alert correlation for supported Dell NAS appliances.

Table 44. Dell NAS Appliance Support

	Dell EqualLogic FS7500 with FluidFS Version 1	Dell EqualLogic FS7500 with FluidFS Version 3	Dell PowerVault MD NX3500 with FluidFS Version 1
Discovery and Classification	Support for discovery using both the EqualLogic Group Manager IP and management IP. If discovered using the controller IPs, it results in multiple entries.	Support for discovery using the controller/node IPs. If discovered using the EqualLogic Group Manager IP, the device will get classified under Dell EqualLogic Group.	Support for discovery using both the controller IPs. If discovered using the PowerVault MD Series array IP, the device is classified as a PowerVault MD Array device.
Appliance Node Information	Displayed in the device inventory.	Displayed in the device inventory.	Displayed in the device inventory.
Alerts	Alerts received from the controller are not correlated to the device.	Alerts received from the controller/node are correlated to the device.  NOTE: It is highly recommended to include all controller/node IP addresses in the discovery range configuration while discovering a NAS cluster with FluidFS version 3.0. This enables OpenManage Essentials to properly associate the SNMP alerts received from various participating controllers/nodes with the discovered cluster.	Some alerts received from the device may be displayed as Unknown.

OEM Device Support

OEM devices (re-branded or de-branded servers and Compellent S8000 iDRAC), when discovered, are classified under **OEM Devices** in the device tree. Most of the functionality available to servers, such as tasks, reports, and filters are also applicable to OEM servers. However, system update may not be possible if it is not supported by the OEM device module. For more information on the supported protocols and features, see information on servers/devices in [Supported Devices Protocols and Features Matrix](#). OEM servers are always classified under the **OEM Devices** group in the device tree. They are not displayed under the **Servers** or **RAC** group. If both the server and RAC of the OEM device are discovered, they are correlated and displayed as one device under the **OEM Devices** group. Other OEM devices except servers and RAC are classified under the different server groups such as Microsoft Virtualization Servers, VMware ESX servers, and so on, based on the classification criteria they satisfy.

 **NOTE: OEM servers discovered using WMI protocol are classified under the Servers device group only when OMSA is installed. OEM servers without OMSA are classified under the Unknown device group.**

Devices — Reference

This page provides the following information:

- List of devices based on the device type, for example, HA clusters, servers, and so on.
- Summary of devices and alerts.
- Alerts generated for a particular device.
- Health of devices based on the Normal, Critical, Unknown, and Warning types.



NOTE: For Dell EMC 12th Generation PowerEdge servers [denoted as $yx2\ x$, where y denotes alphabets, for example M (modular), R (rack), or T (tower) and x denotes numbers] discovered by using WMI and SNMP protocols, the DRAC health status is displayed (under Servers) even if OpenManage Server Administrator is not installed on the server.



NOTE: Based on the severity of the agents of a discovered device, the overall health is the most critical of the severity. For example, in the device tree, for server types, if there are two servers with status Warning and Critical, then the parent Server's status is set to Critical.

- Connection status of devices — When both server (in-band) and DRAC/iDRAC (out-of-band) are discovered and correlated, the **Connection Status** under **Device Summary** displays the connection status of the server. The **RAC Connection Status** under **RAC Device Information** displays the DRAC/iDRAC connection status. When only DRAC/iDRAC (out-of-band) is discovered (server is not discovered), the **Connection Status** and the **RAC Connection Status** display the same information. When only server (in-band) is discovered (DRAC/iDRAC is not discovered), the **Connection Status** displays the connection status of the server. The **RAC Connection Status** is set to **Off**.
- Inventory information for devices.
- View hardware logs for servers.
- Filtering capabilities of the grid:
 - The grouping bar
 - Filter icon options
 - Sorting by clicking on the column
 - Re-ordering the columns



NOTE: None of these are saved if the console is closed and restarted.

Related links

[Viewing devices](#)

[Viewing device inventory](#)

[Creating a New Group](#)

[Adding Devices to an Existing Group](#)

[Hiding a Group](#)

[Using Map View](#)

Viewing Inventory

To view inventory, from **All Devices**, traverse to the device and click the device.

The device details and the alerts link are displayed.

Viewing Alerts

To view alerts, from the inventory details page, click **Alerts**.

Alert Details

Table 45. Alert Details

Field	Description
Severity	Alert severity based on Normal, Critical, Warning, and Unknown.
Acknowledged	Flagged status for an alert.
Time	Time at which the alert was generated in date and time format.
Device	IP address of the device.
Details	Lists the alert information. For example, System is down:<IP Address of the device>
Category	Lists the alert category type, for example System Events.
Source	Lists the alert source name.

Viewing Hardware Logs

You can view hardware logs for servers. To view hardware logs, from the inventory details page, click **Hardware Logs**.

Hardware Log Details

Table 46. Hardware Log Details

Field	Description
Severity	Alert severity based on Normal, Critical, Warning, and Unknown.
Time	The system time at which this alert was generated in date and time format on the managed node.
Details	Lists the details of the hardware log. For example, power supply redundancy is lost.

VLAN Configuration

The **VLAN Configuration** tab allows you to view and manage the VLAN settings of the IOAs within the PowerEdge M1000e and PowerEdge FX2/FX2s chassis.

The following are the fields displayed in the **VLAN Configuration** tab:

Table 47. VLAN Configuration

Field	Description
Last Inventory Time	Displays the last VLAN inventory time.
Grouped by: Fabric	Displays the attribute by which the currently displayed data is grouped. By default, the VLAN configuration inventory is grouped by Fabric .
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Chassis Blade	Displays details of the blade servers that are installed in the chassis.
Modified	Displays if you have modified the VLAN ID.
Server Name	Displays the host name of the blade server.

Field	Description
Service Tag	Displays the Service Tag of the blade server.
Model	Displays the model name of the blade server. If this field is blank, the server is not present.
Slot	Displays the slot where the blade server is installed.
Subslot	Displays the subslot of the blade server node.
NIC	Displays the Fully Qualified Device Descriptor (FQDD) of the NIC.
NIC Port	Displays the NIC port to which the blade server is connected.
Chassis IOA	Displays details of the IOAs that are installed in the chassis.
IOA Name	Displays the name of the IOA.
IOA Model	Displays the model name of the IOA.
Fabric	Displays the fabric associated with a specific slot of the chassis. The fabric is identified by a combination of the group name (A, B, or C) and slot number (1 or 2).
Port	Displays the port assigned to the IOA.
Tagged VLAN(s)	Displays the tagged VLAN IDs of the IOAs.
Untagged VLAN	Displays the untagged VLAN IDs of the IOAs.
Set to default value	Click to set the VLAN IDs to the default values.
Reset All	Click to revert all changes that you had made.
Apply	Click to apply the changes to the VLAN settings.

VLAN Configuration Task

The **VLAN Configuration Task** window is displayed when you click **Apply** to assign VLAN IDs. The following are the fields that are displayed in the **VLAN Configuration Task** window:

Table 48. VLAN Configuration Task

Field	Description
Task Name	Displays the name of the VLAN configuration task.
Selected IO Module Ports	Displays the IOA ports that you have selected to apply changes.
Grouped by: Fabric	Displays the attribute by which the currently displayed data is grouped. By default, the VLAN configuration inventory is grouped by Fabric .
Chassis Blade	Displays details of the blade servers that are installed in the chassis.
Server Name	Displays host name of the blade server.
Service Tag	Displays the unique identifier assigned to the blade server.
Model	Displays the model name of the blade server.
Slot	Displays the slot where the server is installed.
Subslot	Displays the subslot of the server node.






Field	Description
NIC	Displays the Fully Qualified Device Descriptor (FQDD) of the NIC.
NIC Port	Displays the NIC port to which the server is connected.
Chassis IOA	Displays details of the IOAs that are installed in the chassis.
IOA Name	Displays the name of the selected IOA.
IOA Model	Displays the model name of the selected IOA.
Fabric	Displays the fabric associated with a specific slot of the chassis. The fabric is identified by a combination of the group name (A, B, or C) and slot number (1 or 2).
Port	Displays the port assigned to the IOA.
Tagged VLAN(s)	Displays the list of tagged VLANs for the selected IOA.
Untagged VLAN	Displays the untagged VLAN for the selected IOA.
Set the Task Schedule	
Run now	Select to run the configuration task immediately.
Set Schedule	Select to schedule a task at a required date and time.
Enter IOA Credentials for the task execution	
User Name	Provide the fabric administrator user name required to run the task.
Password	Provide the fabric administrator password required to run the task.
Help	Click to open the online help.
Cancel	Click to cancel the task.
Finish	Click to run the task at the defined schedule.

Task Results

The **Task Results** tab displays the status of tasks.

The following table describes the fields that are displayed in the **Task Results** tab.

Table 49. Task Results

Field	Description
Status	Displays an icon representing the task status:  — Running or pending  — Complete  — Stopped  — Failed  — Warning
Task Name	Displays the name of the task.
Start Time	Displays the start time of the task.

Field	Description
% Completed	Displays the progress information of the task.
Task State	Displays the state of the task: <ul style="list-style-type: none"> Running Complete Stopped Failed Warning
End Time	Displays the end time of the task.
Executed by User	Displays the name of the user who executed the task.

Alert Filters

You can apply these filters to Alerts. Select **Continuous Updates** to enable the user interface to update automatically when new alerts are received.

Table 50. Alert Filters

Field	Description
Severity	Select from these alerts: All, Normal, Critical, Warning, and Unknown.
Acknowledged	Flagged status for an alert.
Time	Time at which this alert was generated in date and time format.
Device	The IP address or host name of this device.
Details	The alert information. For example, System is down: <IP address of the device>.
Category	The alert category type, for example System Events.
Source	The Alert Source.

Viewing noncompliant systems—Devices

To view noncompliant systems associated with

- A catalog baseline, click the **Non-Compliant Firmware & Drivers** tab.
- A configuration baseline, click the **Non-Compliant Configurations** tab.



NOTE: Non-compliant systems are only available for device groups such as servers, RAC, and custom groups. It is not available for individual devices.

Non-Compliant Firmware and Drivers

The Non-Compliant Firmware & Drivers tab provides the following information:

Table 51. Non-Compliant Firmware & Drivers

Field	Description
System Name	Domain name of the system.
Group Name	Displays the name of device groups.

Field	Description
Baseline Name	Displays the name of catalog baseline associated with a device group.
Model Type	The systems model name. For example, PowerEdge.
Operating System	The operating system that is installed on the system.
Service Tag	A unique identifier, that provides the service lifecycle information.
Update Method	Displays the update methods such as OpenManage Server Administrator and iDRAC.
Discovered Time	Time and date of discovery.
Inventory Time	Time and date of inventory.

Select noncompliant systems, and select the updates in the **Select Updates to Apply** pane. Click **Apply Selected Updates**.

Table 52. Apply Selected Updates

Field	Description
System Name	System's domain name.
Importance	The requirement of this software update for the system.
Update Method	Displays the update methods such as OpenManage Server Administrator and iDRAC.
Component	The software information.
Type	The type of software update.
Installed Version	The installed version number.
Upgrade/Downgrade	A green arrow indicates an upgrade.
Available Version	The available version number.
Package Name	The name of the software update.
Reboot Required	Specifies whether the update requires a system reboot.

Related link

[System Update](#)

Non-Compliant Configurations

Table 53. Non-Compliant Configurations

Field	Description
Device Name	Displays the name of the device.
Service Tag	A unique identifier, that provides the service lifecycle information.
Model	The model name of the system. For example, PowerEdge.
Compliance Baseline	The configuration baseline associated with the device.
Inventory Last Run	Time and date of inventory.

Device Search

The search options available are:

- Run an existing query
- Create a new query
- Delete a query

Table 54. Device Search

Field	Description
Run Existing Query	Select this option and then select a query from the drop-down list.
Delete Query	Select to delete a query after you complete the following action. Select the Run Existing Query option, then from the drop down list select the query that you want to delete.
Create New Query	Select this option to create a query and then enter a name for the query in the adjoining field.
Query logic	Select from the query logic options to create multiple query options. Select the check box to enable and include an argument.
Run Query	Runs the selected query.
Save Query	Saves the selected query.

Related link

[Query Results](#)

Query Results

The device search lists these options:

Table 55. Query Results

Field	Description
Health Status	Displays the health status of the device. The status options are Normal , Warning , Critical , and Unknown .
Connection Status	Displays the connection status of the device. The connection status are On or Off .
Name	Displays the name of the device.
OS Name	Displays the operating system installed on the device.
OS Revision	Displays the version of the operating system installed on the device.
Service Tag	Displays a unique identifier, that provides the service lifecycle information.
Asset Tag	Displays the defined asset tag for the device.
Device Model	Displays the system's model name. For example, PowerEdge R710.
Device type	Displays the type of device. For example, for the Device Model PowerEdge R710, the Device Type value is Server.
System Revision Number	Displays the revision history of the device.

Creating Device Group

Device Group Configuration

Table 56. Device Group Configuration

Field	Description
Name	Provide name of the new group.
Parent	The device under which this group is created.
Description	Provide description for the device group.

Device Selection

You can select predefined groups (device types), custom groups, specific devices, or a device query.

To use device query, select a query from the list.

Click **New** to create a new device query to search and assign the devices to the alert action.

Click **Edit** to change the query logic.

Select groups or devices from the tree, you can use the query option to create very specific criteria for the selection.

Device Selection Options

Table 57. Device Selection Options

Field	Description
All Devices	Select to include all the devices that are managed in OpenManage Essentials.
Citrix XenServers	Select to include Citrix XenServers.
Clients	Select to include client devices, such as desktops, portables, and workstations.
Hyper-Converged Infrastructure	Select to include VxRail and XC Series devices.
HA Clusters	Select to include High Availability server clusters.
KVM	Select to include keyboard video mouse devices.
Microsoft Virtualization Servers	Select to include Microsoft virtualization servers.
Modular Systems	Select to include modular systems.
Network Devices	Select to include network devices.
OOB Unclassified Devices	Select to include out of band Unclassified Devices like Lifecycle Controller enabled devices.
Power Devices	Select to include PDUs and UPS.
PowerEdge C Servers	Select to include PowerEdge C servers.
Printers	Select to include printers.
RAC	Select to include devices with remote access controllers.
Servers	Select to include servers.
Storage Devices	Select to include storage devices.
Unknown	Select to include unknown devices.
VMware ESX Servers	Select to include VMware ESX servers.

Field	Description
VxFlex Ready Nodes	Select to include VxFlex Ready Nodes and ScaleIO Ready Nodes.




Summary — Group Configuration

View and edit selections.

Map View Interface—Devices Tab

The following are the items displayed in the **Map View** and their descriptions.

Table 58. Map View (Devices) Tab Interface

Item	Description
Search bar	Enables you to search for locations on the map.
Internet connection warning  NOTE: The Internet connection warning is displayed only if the Show internet connection warning when unable to connect to the internet option is selected in Map Settings.	Indicates if the system is not connected to the Internet.
Overlays menu	Enables you to overlay the health or connection status of the device on the pin. The options available are: <ul style="list-style-type: none"> • Health • Connectivity A tick mark is displayed beside the option that is selected.
Actions menu	Enables you to select a list of actions that can be performed. The available actions are: <ul style="list-style-type: none"> • Show All Map Locations • Go to Home View • Save Current View as Home View • Add Licensed Device • Import Licensed Devices • Remove All Map Locations • Export • Settings • Edit Location Details • Remove Location • Zoom to Street Level  NOTE: The Zoom to Street Level option is displayed only when a device is selected on the map.  NOTE: The Edit Location Details, Remove Location, and Zoom to Street Level options in the Actions menu are device-specific. These options must be used after selecting a device on the map.
Navigation toolbar	Enables you to move the map, zoom in or zoom out, and select a map service provider. The options available map providers are:

Item	Description
	<ul style="list-style-type: none"> • MapQuest Provider (Licensed) • Bing Road Provider (Licensed) • Bing Satellite Provider (Licensed)
Scale	Displays the current zoom level of the map in meters or kilometers.

Devices at this location

The **Device at this location** window is displayed when you double-click or right-click a multi-pin group and then select **Details**. The following are the fields displayed in the **Devices at this location** window:

Table 59. Devices at this location

Field	Description
Health Status	Displays the health status of the device. The status options are Normal , Warning , Critical , and Unknown .
Connection Status	Displays the connection status of the device. The connection statuses are On or Off .
Device Name	Displays the name of the device.
Service Tag	Displays a unique identifier, that provides the service lifecycle information.
Asset Tag	Displays the defined asset tag for the device.
Model	Displays the model name of the system. For example, PowerEdge R710.
Description	Displays the description of the device.
Address	Displays the location information of the device.
Contact	Displays the contact information of the device.

Map Settings

The following table provides information about the fields displayed in the **Map Settings** dialog box.

Table 60. Map Settings

Field	Description
Update map view on any device or device group selection	Select to configure the map to display only the pin or pins that correspond to the device or device group selected in the device tree.
Show internet connection warning when unable to connect to the internet	Select to display a message on the map when an Internet connection is not available.
Bing Key	Select to provide a valid Bing key required by the Bing map provider.
MapQuest Key	Select to provide a valid MapQuest key required by the MapQuest map provider.
Key	Allows you to enter a valid Bing key or MapQuest key for rendering the Map View.
Cancel	Click to close the Map Settings dialog box.

Field	Description
Apply	Click to save the updates in the Map Settings dialog box.

Related link

[Using Map View](#)

Deployment and reprovisioning

Every server and chassis has a large list of attribute values that describe the settings and functionality of the device. These settings must be set properly before deploying an operating system to make the server functional. The **Deployment Portal** enables you to perform initial server or chassis configuration and operating system deployment. The portal allows you to create a server or chassis configuration templates that include settings for Lifecycle Controller system, iDRAC, BIOS, RAID, NIC for servers, and CMC for chassis. These configuration templates can then be deployed to multiple servers or chassis for initial configuration before an operating system deployment process is kicked off from a predefined bootable ISO image.


Using the **Deployment Portal**, you can:

- Create a device configuration template
- Edit a device configuration template
- Create a chassis infrastructure template
- Add devices to the repurpose and bare-metal group
- Modify or remove devices from the repurpose and bare-metal group
- Deploy a bare-metal server
- Create a virtual I/O identity pool
- Create a compute pool
- Deploy a server with virtual I/O identities (stateless deployment)
- Replace a server
- View the tasks that have been created and their status
- Configure the deployment file share

 **NOTE: In OpenManage Essentials version 2.5, streaming functionality is used for the device configuration deployment and configuration compliance tasks of:**

- PowerEdge servers with the latest version of iDRAC7 or 8, and firmware versions of 2.50.50.50 and later installed.
- PowerEdge servers with the latest version of iDRAC9, and firmware versions of 3.00.00.00 and later installed.

It is recommended to upgrade the servers to the latest firmware versions, and avoid using file share settings because of security reasons in the Windows operating systems.

 **NOTE: Devices in the repurpose and bare-metal group are displayed as targets for device configuration deployment. You must explicitly add devices to the repurpose and bare-metal group for deploying a device configuration. On bare-metal deployments, you can remove the devices from the repurpose and bare-metal group after the deployment is complete.**


 **NOTE: The device configuration deployment and configuration compliance features are licensed (fee-based) for supported PowerEdge servers with iDRAC. The CMC Enterprise License is required for creating and deploying device configuration along with verifying configuration compliance on PowerEdge VRTX and PowerEdge FX2/FX2s chassis. For more information about licensing, see [OpenManage Essentials — Server Configuration Management License](#).**

 **NOTE: No license is required for creating or deploying device configuration on PowerEdge M1000e chassis or IOA.**


Related links


[Configuring the deployment file share](#)
[Creating a device deployment template](#)
[Adding devices to repurpose and bare-metal devices group](#)
[Managing device deployment templates](#)
[Deploying a device deployment template—Bare-metal deployment](#)
[Deploying a device configuration template—Stateless deployment](#)
[Deploying a network ISO image](#)
[Auto deploying device configurations](#)
[Viewing the Deployment Tasks](#)
[Additional information](#)

Server Configuration Management license

 **NOTE:** Installing and using OpenManage Essentials does not require the Server Configuration Management license. The server configuration management feature requires the Server Configuration Management license be installed on target servers.

The Server Configuration Management license enables you to deploy a device configuration and verify device configuration compliance on licensed servers. The license is a perpetual license that is valid for the life of a server, and can be bound to the Service Tag of only one server at a time.

 **NOTE:** Enabling the server configuration management feature in OpenManage Essentials does not require any separate license. If the Server Configuration Management license is installed on a target server, you can use the server configuration management feature on that server.

 **NOTE:** The Server Configuration Management license is required only for deploying device configurations and verifying configuration compliance on servers, and this license is not required for creating device configuration template from a server.

Licensable servers

You can apply Server Configuration Management license to the following servers:

- PowerEdge servers having iDRAC7 with firmware version 1.57.57 or later
- PowerEdge servers having iDRAC8 with firmware version 2.00.00.00 or later
- PowerEdge servers having iDRAC9 with firmware version 3.00.00.00 or later

Purchasing license

You can purchase the Server Configuration Management license when you purchase a server or by contacting your Sales Representative. You can download the purchased license from the Software License Management Portal at Dell.com/support/retail/lkm.

Deploying the license

If you purchase a license after you have purchased a server, you can deploy the license on the server using the Dell EMC License Manager. You can install License Manager using the OpenManage Essentials installation package. For information about deploying the license, see the *Dell EMC License Manager User's Guide* at Dell.com/OpenManageManuals.

Verifying license information

You can verify if the Server Configuration Management license is installed on a server through one of the following methods:

- In the **Reports** portal, **Managed Systems Reports > Warranty & License**, click **License Information**. The **License Description** column indicates the license that has been installed on the licensed devices.

- Select a device in the device tree. The **License Information** table in the device inventory indicates the licenses installed on the device.

Viewing unlicensed server targets

To view the server targets for configuration management that do not have the Server Configuration Management license installed:

1. Navigate to the **Manage > Configuration > Device Configuration Compliance Portal**.
2. In the **Device Compliance** pie-chart, click the **Non-licensed** segment. All the **Non-licensed Devices** window displays the possible targets for server configuration management that do not have a license.

Related links

[Deploying a device deployment template—Bare-metal deployment](#)
[Deploying a device configuration template—Stateless deployment](#)
[Setting up device configuration auto deployment—Bare-metal deployment](#)
[Setting up device configuration auto deployment—Stateless deployment](#)
[Configuring the credentials and device configuration inventory schedule](#)

Device requirements for deployment and compliance tasks

The following are the device requirements for device configuration deployment and configuration compliance tasks:

- For servers:
 - PowerEdge servers with the latest version of iDRAC7, 8, or 9 with the Lifecycle Controller firmware installed.
 - Server Configuration Management license installed on the iDRAC. This license is not the same as the iDRAC license.
 - iDRAC Enterprise or iDRAC Express license. This license is not the same as the Server Configuration Management license. If the iDRAC Enterprise license is not installed on target servers, certain features of iDRAC are not available.
- For chassis:
 - Supported firmware versions:
 - PowerEdge MX7000—firmware version 1.0 and later installed.
 - PowerEdge M1000e—firmware version 6.1 and later installed.
 - PowerEdge VRTX—firmware version 3.1 and later installed.
 - PowerEdge FX2 or FX2s—firmware version 2.1 and later installed.
 - PowerEdge FX2, FX2s, and VRTX chassis must have an Enterprise license.
- For IOAs:
 - IOAs must be configured in one of the following operational modes:
 - Standalone
 - Virtual Link Trunk (VLT)
 - Programmable MUX (PMUX)



NOTE: Compliance tasks are not supported for IOAs and IOA attributes in the chassis templates.

- The IO aggregator must have firmware version of 9.10.0.0, 9.10.0.1P10, 9.11.0.0, 9.11.2.0, 9.13.0.0, and 9.14.0.0 installed.

Related links

[Creating a device deployment template from a device configuration file](#)
[Creating a device deployment template from a reference device](#)
[Deploying a device deployment template—Bare-metal deployment](#)
[Deploying a device configuration template—Stateless deployment](#)
[Deploying a network ISO image](#)
[Setting up device configuration auto deployment—Bare-metal deployment](#)
[Configuring the credentials and device configuration inventory schedule](#)
[Viewing the device configuration inventory](#)

Getting started for device configuration deployment

Before you deploy a device configuration to target devices, you must:

1. Configure the deployment file share on the server running OpenManage Essentials.



NOTE: In OpenManage Essentials version 2.5, streaming functionality is used for the device configuration deployment and configuration compliance for the following devices:

- PowerEdge servers with the latest version of iDRAC7 or 8, and firmware versions of 2.50.50.50 and later installed.
- PowerEdge servers with the latest version of iDRAC9, and firmware versions of 3.00.00.00 and later installed.



NOTE: It is recommended to upgrade the servers to the latest firmware versions, and avoid using file share settings due to security reasons in the Windows operating systems.

2. Add target devices to the repurpose and bare-metal group.

Related links

[Overview of bare-metal deployment](#)
[Overview of Stateless Deployment](#)
[Configuring the deployment file share](#)
[Adding devices to repurpose and bare-metal devices group](#)

Viewing the Deployment Portal

To view the deployment portal, click **Deployment** → **Deployment Portal**.

Configuring the deployment file share

Before creating or deploying a configuration template from a chassis, you must configure the deployment file share in OpenManage Essentials. However, configuring deployment file share for iDRAC devices is optional. iDRAC with the latest firmware version uses streaming functionality for creating or deploying a configuration template. The deployment file share temporarily stores the configuration file that retrieves and applies the configuration settings on a target server or chassis.

To configure the deployment file share:

1. Perform one of the following:
 - Click **Settings** → **Deployment Settings**.
 - Click **Deployment**. In the **Common Tasks** pane, click **File Share Settings**.
 - Click **Deployment** → **Getting Started for Deployment** → **Configure Deployment File Share**.
 - Click **Manage** → **Configuration**. In the **Common Tasks** pane, click **File Share Settings**.

The **File Share Settings** window is displayed.

2. Type the domain\user name and password of the server that is running OpenManage Essentials.
3. If not selected by default, select the **Allow using the file share for Device Configuration feature on server** check box.
4. Click **Apply**.

A warning message is displayed indicating that you must upgrade to the latest firmware version which uses the streaming functionality. Indicate your confirmation to proceed.


The deployment file share is now configured.


Related link

[Getting started for device configuration deployment](#)

Adding devices to repurpose and bare-metal devices group

Adding devices to the **Repurpose and Bare Metal Devices** group is a prerequisite for deploying either a configuration template or a network ISO image on those devices.

 **CAUTION:** Ensure that only the appropriate devices are added to the repurpose and bare-metal devices group. After deploying a configuration template on a repurpose and bare-metal device, it may not be possible to revert the device to its original configuration.

 **NOTE:** Servers that you want to add to the Repurpose and Bare Metal Device Group must have the Server Configuration Management license installed. For more information, see [OpenManage Essentials — Server Configuration Management License](#).

To add devices to the repurpose and bare-metal devices group:

1. Click **Deployment** → **Deployment Portal**.
2. In the **Repurpose and Bare Metal Devices** tab, click **Modify Devices**.
The **Modify Devices of the Repurpose and Bare Metal Device Group** window is displayed.
3. From the **All Applicable Devices** tree, select the devices that you want to add to the **Repurpose and Bare Metal Devices** group.
4. Click **Finish**.
The devices are listed in the **Repurpose and Bare Metal Devices** tab in the right pane, and in the **Repurpose and Bare Metal Devices** group in the device tree.

Related links

[Deploying a device deployment template—Bare-metal deployment](#)


[Getting started for device configuration deployment](#)

[Repurpose and Bare Metal Devices](#)

Overview of bare-metal deployment

The steps that you must perform to deploy a device configuration template on target devices are as follows:

1. **Create a device configuration template**—Use the **Create Template** task in the **Common Tasks** pane to create a device configuration template. You can choose to create the template from either a configuration file or a reference device.
2. **Edit the device configuration template**—Select the template from the **Templates** pane, and edit the desired configuration attributes displayed in the right pane.
3. **Deploy the device configuration template on target devices**—Use the **Deploy Template** task in the **Common Tasks** pane to select the template, target devices, edit device-specific attributes, and then deploy the configuration attributes. You can also use the **Setup Auto Deployment** task to deploy a device configuration template on devices that you will be discovering later.

 **NOTE:** If the hardware of the device from which the device configuration template was created and the hardware of the deployment targets are identical, it enhances the possibility of the attributes being deployed successfully. If the hardware is not entirely identical, the deployment task may not complete successfully. However, the attributes for the matching components are deployed successfully.

Related links

- [Getting started for device configuration deployment](#)
- [Creating a device deployment template](#)
- [Editing a device deployment template](#)
- [Deploying a device deployment template—Bare-metal deployment](#)

Creating a device deployment template

The **Create Template** task creates a device deployment template that includes the attributes of a server, chassis, or an IOA. Using the device deployment template, you can:

- Deploy the configuration on another server, chassis, or an IOA.
- Create a chassis infrastructure configuration template.
- Verify the compliance of either a server or chassis to the configuration baseline.



NOTE: Compliance tasks are not supported for IOA templates.

You can create a device deployment template from:

- A device configuration file.
- A server or chassis that you have discovered.

Related links

- [Creating a device deployment template from a device configuration file](#)
- [Creating a device deployment template from a reference device](#)

Creating a device deployment template from a device configuration file

You can create a device deployment template from an existing server or chassis configuration (.xml) file, or IOA configuration (.txt) file.

Before you create a deployment template from a device configuration file, ensure that:

- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- The configuration file is from a device that meets the requirements specified in [Device Requirements for Deployment and Compliance Tasks](#).
- For IOA templates only—Ensure that the IOA template that you want to import has not been edited after it was created. Editing an IOA template, compromises the integrity of the template. Therefore, deploying the edited IOA template results in a failure.

To create a device deployment template from a device configuration file:

1. Click **Deployment** → **Deployment Portal**.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Create Template**.
 - In the **Templates** pane, right-click **Server Template**, **Chassis Template**, or **IOA Template**, and then click **Create Template**.
 - In the **Common Tasks** pane, click either **Getting Started for Deployment** or **Getting Started for Compliance** → **Create Template**.

The **Create Template Wizard** is displayed.



NOTE: If the deployment file share settings are not configured, a message stating that One or more settings require configuring for this action is displayed. If you click OK, the File Share Settings window is displayed. After you configure the file share settings, the Create Template Wizard is displayed.

3. In the **Name** field, enter a name for the template.
4. Click **Create from File**.
5. Click **Browse**.

6. Navigate and select the configuration file, and then click **Open**.
7. Click **Finish**.

The deployment template that is created is displayed in the **Templates** pane.

 **NOTE:** IOA templates can only be created and deployed. The IOA templates that you create are displayed only in the **Deployment Portal**.

Related links

[Create Template Wizard](#)

[Device requirements for deployment and compliance tasks](#)

Creating a device deployment template from a reference device


You can create a device deployment template from a server, chassis, or an IOA that you have discovered in OpenManage Essentials. Before you create a deployment template from a reference device, ensure that:

- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- You are creating a device configuration template from a device that meets the requirements specified in [Device Requirements for Deployment and Compliance Tasks](#).

To create a device deployment template from a reference device:

1. Click **Deployment** → **Deployment Portal**.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Create Template**.
 - In the **Templates** pane, right-click **Server Template**, **Chassis Template**, or **IOA Template**, and then click **Create Template**.

The **Create Template** window is displayed.

 **NOTE:** If the deployment file share settings are not configured, a message stating that **One or more settings require configuring for this action is displayed**. If you click **OK**, the **File Share Settings** window is displayed. After you configure the file share settings, the **Create Template Wizard** is displayed.

3. Enter a name for the template.
4. Select the device type (**Server**, **Chassis**, or **IOA**) and perform one of the following:
 - Select a device from the **All Applicable Devices** tree.
 - Search for a device by using the **Search Devices** box.

 **NOTE:** In the **Create Template Wizard**, under **All Applicable Devices** tree, all the devices discovered and inventoried are listed. The devices without an enterprise license and supported firmware are disabled and cannot be selected.

5. Under **Execution Credentials**, provide the device credentials that have Administrator rights, and click **Finish**.
6. In the task submission message, click **Ok**.

A **Create Template** task is created in the **Tasks** tab in the right pane. You can view the status of the deployment template in **Task Execution History** in the right pane. You can double-click the task in **Task Execution History** to view the task execution details. The template that is created is displayed in the **Templates** pane.

 **NOTE:** IOA templates can only be created and deployed. The IOA templates that you create are displayed only in the **Deployment Portal**.

Related links

[Create Template Wizard](#)

[Device requirements for deployment and compliance tasks](#)

Managing device deployment templates

The device deployment templates contain various attributes of a server, chassis, or IOA. Before you use the template for deployment, you can:

- View the attributes of a device deployment template.
- Clone a device deployment template.
- Edit a device deployment template.
- Export a device deployment template.
- View the properties of a device deployment template.

Related links

[Viewing device deployment template attributes](#)

[Cloning a device deployment template](#)

[Editing a device deployment template](#)

[Exporting a device deployment template](#)


Viewing device deployment template attributes

1. Click **Deployment** → **Deployment Portal**.
2. In the **Templates** pane, click either a sample template or a template that you created.

The attributes of the template are displayed in the **Attributes** tab in the right pane. The total number of attributes in the template is displayed at the upper right of the **Attributes** tab.

 **NOTE: The device-specific attributes and virtual I/O identity attributes of a device deployment template can only be viewed in the Edit Attributes tab of the Deploy Template Wizard.**

 **NOTE: IOA templates can only be created and deployed. The IOA templates that you create are displayed only in the Deployment Portal.**

 **NOTE: If the device deployment template was created from a blade server, the right pane also displays the IOA VLAN Attributes tab. This tab contains the VLAN attributes that you can deploy on the IOA while deploying a blade server.**

Related links

[Managing device deployment templates](#)

[Device Configuration Template Details](#)

Cloning a device deployment template

You can clone a device deployment template to create a template that you can edit and deploy.

To clone a device deployment template:

1. Click **Deployment** → **Deployment Portal**.
2. In the **Templates** pane, right-click a template, and then click **Clone**.
The **Clone Configuration Template** window is displayed.
3. Enter a name for the template, and click **Ok**.

The cloned template is displayed in the **Templates** pane under the sample templates.

Related link

[Managing device deployment templates](#)

Editing a device deployment template

You can edit a device deployment template to change the values of the attributes before you deploy on the target devices.

 **NOTE: Editing of an IOA template is not supported.**

To edit a device deployment template:

1. Click **Deployment** → **Deployment Portal**.
2. In the **Templates** pane, right-click a template, and then click **Edit**.
3. The boot configurations and the network interface settings are displayed in the **Boot and Network Configuration** tab in the right pane. Under **First Boot Configuration**, select the boot mode and the boot type.

 **NOTE: The default boot type is selected based on the boot type that is specified in the captured template.**


If **FC** is selected as the boot type, then enter details in the following fields:

- a. **First Target WWPN**—the WWPN address
- b. **First Target LUN Id**—the LUN ID for the first target
- c. **Second Target WWPN**—the WWPN address
- d. **Second Target LUN Id**—the LUN ID for the second target.

If **FCoE** is selected as the Boot Type, then enter details in the following fields:

- a. **First Target WWPN**—the WWPN address
 - b. **First Target LUN Id**—the LUN ID for the first target
4. Click **More Settings** to change the boot sequence and the hard drive sequence.
 5. Under **Network Interface Settings**, all the network interfaces settings available in the selected template are displayed.
 - a. If the partitioning is supported, then enable the partitioning and provide the **Minimum Bandwidth (%)** and **Maximum Bandwidth (%)**.
 - b. For the templates captured from the modular servers, provide the **Tagged VLAN(s)** and the **Untagged VLAN** values for the IOA ports under **Integrated NIC**.
 6. Click **Save**.

The values that are provided in the **Tagged VLAN(s)** and the **Untagged VLAN** fields are displayed in the **IOA VLAN Attributes** tab.
 7. The attributes of the template are displayed in the **Attributes** tab in the right pane. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target device, clear the check box for that attribute in the **Deploy** column.
 8. To select or clear all the attributes in the template, select or clear the check box that is displayed next to the **Deploy** column title.

 **NOTE: If the value of an attribute depends on another attribute, the dependency is indicated in the Dependencies column of the configuration template. To deploy the dependent attributes, you must first edit the primary attributes, and then edit the dependent attribute.**

9. To select multiple rows of attributes, select the row that has the first attribute, press and hold the <Shift> key, and click the row that has the last attribute. To select or clear the attributes of the selected rows, right-click and select **Check** or **Uncheck**.
10. Edit or select the values in the **Value** column based on your preference.

The total number of attributes in the template and the number of attributes that you edit are displayed in the upper right of the **Attributes** tab.

11. To configure network and VLAN settings for the compute sleds in a MX7000 chassis:

- a. To configure a network:
 1. Click **MX Chassis Networks** → **Add New**.
 2. Enter a name, description, and a valid VLAN ID for the network.
 3. Select a network type from the drop-down list and click **Ok**. For more information about the available network types, see [Network Types](#).
 4. To save the configured network attributes, click **Save**, and then click **Yes** to confirm.

- b. To assign IOA ports to the configured VLANs:
 1. Click **VLAN Configuration**.
 2. Select the port, and then assign the Tagged and Untagged VLANs.
 3. To save the VLAN attributes, click **Save**, and then click **Yes** to confirm.

12. Click **Save**.

Related link

[Managing device deployment templates](#)

Exporting a device deployment template

You can export a device deployment template to an XML (server configuration template) or an INI (chassis configuration template) file. Exporting the attributes enables you to use an alternative method to edit the attributes. After editing the template, you can import the template and use it for deployment.

To export a device deployment template:

 **NOTE:** Exporting a device template exports all the attributes of the template, including attributes that are not selected.

1. Click **Deployment** → **Deployment Portal**.
2. In the **Templates** pane, right-click either a sample template or a template that you created, and then click **Export Template**.
3. Navigate to the location where you want to export the template, provide a filename, and then click **Save**.

Related link

[Managing device deployment templates](#)

Deploying a device deployment template—Bare-metal deployment

The **Deploy Template** task allows you to deploy a configuration template that includes a set of configuration attributes to specific devices. Deploying a device configuration template on the devices ensures that the devices are uniformly configured. Bare-metal servers and chassis are devices that only have basic iDRAC communication configured and are not yet provisioned for operations.

Before you begin deploying a device deployment template, ensure that:

- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- The target devices are added to the repurpose and bare-metal group, or a compute pool. For more information, see [Adding Devices to the Repurpose and Bare Metal Devices Group](#).
- You have either created a device deployment template or cloned a sample template.
- The target devices meet the requirements specified in [Device Requirements for Deployment and Compliance Tasks](#).
- The Server Configuration Management license is installed on all target servers. For more information, see [OpenManage Essentials — Server Configuration Management License](#).
- For IOA VLAN configuration deployment, the template must be created from a blade server.

 **NOTE:** Dell EMC recommends that you deploy the configuration templates that are captured from a server with BOSS-S1 AHCI controller as-is without editing the attributes.

 **CAUTION:** Deploying a configuration template on a device may result in potentially destructive changes to the device configuration including performance, connectivity, and ability to boot the device.

To deploy the configuration template on bare-metal devices:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Deploy Template**.
 - In the **Compute Pools** pane, right-click the compute pool that has the target devices, and then click **Deploy**.

The **Deploy Template Wizard** wizard is displayed.

3. On the **Name and Deploy Options** page:
 - a. Enter an appropriate name for the task.
 - b. Under **Deploy Target**, select **Bare Metal**.
 - c. Under **Select Deploy Options**, select **Deploy Template**.

 **NOTE:** If you want to deploy a configuration template and then boot the device to a network ISO image, you can select both **Deploy Template** and **Boot to Network ISO**. Separate tasks are created for each operation.

- d. Click **Next**.

4. On the **Select Template** page:
 - a. Based on the target device type, click **Server Template** or **Chassis Template**.
 - b. Select the configuration template you want to deploy.

 **NOTE:** Only configuration templates that you have either created or cloned are available for selection.


- c. Click **Next**.

5. On the **Select Virtual I/O Pool** page, click **Next**.

6. On the **Select Devices** page, select the target devices from the **Repurpose and Bare Metal Devices** tree, and click **Next**.

 **NOTE:** Only devices added to the repurpose and bare-metal group that are not assigned to a compute pool are available for selection.

7. On the **Edit Attributes** page:

 **NOTE:** OpenManage Essentials does not include any passwords from the source when the configuration template is created. If you want to set the passwords for the target devices, all password attributes must be edited in the configuration template before deployment. If you want to change the password, ensure to run the deployment task as a different user. If you are changing the password of the device through the deployment, ensure that you run the deployment task with a different user account.


- a. Click the **Template Attributes** tab.
 - b. Click the attribute group name to view the list of attributes in a group.
 - c. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target device, clear the check box in the **Deploy** column.
 - d. Edit or select the values in the **Value** column based on your preference.

The total number of attributes in the template and the number of attributes that you edit are displayed in the **Grouped by** bar.


- e. Click **Save**.
 - f. Click the **Device Specific Attributes** tab to edit the attributes that are unique for the target device.

 **NOTE:** The **Device Specific Attributes** tab may or may not display attributes based on the template selected for deployment.

- g. Click the attribute group name to view the list of attributes in a group.
 - h. To assign a new Static IPv4 Address for the deployment, enter the Static IPv4 Address in the **Value** column of **IPv4Static 1 IPv4 Address** attribute.

 **NOTE:** Deploying the template with the changed Static IPv4 Address initiates a new discovery task for the device. For more information on the task details, see [Task Status](#). The new Static IPv4 Address is added to the discovery range under **Manage** → **Discovery and Inventory** → **Discovery Ranges** → **All Ranges**.

 **NOTE:** If Static IPv4 Address is used in the deployment of a chassis template, then all the components in the chassis are rediscovered after the deployment task is completed.

 **NOTE:** If Static IPv4 Address is provided and the DHCP attribute is enabled, then the DHCP settings take precedence over the provided Static IPv4 address. Similarly, If Static IPv4 Address is provided and the DHCP attribute is disabled, then the Static IPv4 Address is used for the template deployment.

- i. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target device, clear the check box in the **Deploy** column.
 - j. Edit or select the values in the **Value** column based on your preference.
 - k. Click **Save**.

- l. (For IOA VLAN configuration deployment only) Click the **IOA VLAN Attributes** tab to view the IOA VLAN attributes for the selected template.
- m. Click **Next**.
8. On the **Set Schedule** page:
 - a. Select either **Run now**, or click the calendar icon and select the date and time you want to run the task.
 - b. Under **Execution Credentials**:
 - For server configuration deployment — type the credentials that have Administrator privileges on the iDRAC of the target servers.
 - For chassis configuration deployment — type the credentials that have Administrator privileges on the CMC of the target chassis.
 - c. (Only for IOA VLAN configuration deployment) Under **IOA Credentials**, type the credentials that have Administrator privileges on the IOA.
 - d. Click **Next**.
9. On the **Preview** page:
 - a. Optional: Click **Preview** to verify if the attributes of the device configuration template will be deployed successfully on the target devices.
 - b. Click **Next**.
10. On the Summary page, review the information that you have provided, and then click **Finish**.
The **Deploy Template** warning is displayed.
11. If you want to continue the deployment, click **Yes**.

The Deploy Template task is created and run based on the schedule you have selected. You can double-click the task in **Task Execution History** to view the task execution details.

The Deploy Template task fails if:

- The file share setting is not enabled for servers with unsupported firmware versions installed.
- The streaming functionality is disabled on target servers and if the file share setting is not enabled on OpenManage Essentials.


 **NOTE:** In OpenManage Essentials 2.5, the device configuration deployment by using the streaming functionality is taking longer than deploying by using the file share setting. The following table lists the time taken for the device configuration deployment tasks to complete in an environment with 1–100 devices by using the file share and streaming functionality:

Table 61. Time taken by the device configuration deployment task

Number of device(s)	Time required for configuration deployment by using the file share and iDRAC 2.41.40.40 when...		Time required for configuration deployment by using the streaming functionality and iDRAC 2.52.52.52 when...	
	Devices are turned off	Devices are turned on	Devices are turned off	Devices are turned on
1	2 minutes 30 seconds	1 minute 50 seconds	5 minutes 40 seconds	2 minutes 10 seconds
50	2 hours	1 hour 30 minutes	3 hours	2 hours
100	5 hours 20 minutes	3 hours 40 minutes	7 hours	4 hours 30 minutes

Related links

[Deploy Template Wizard](#)
[Device Configuration Setup Wizard](#)
[Server Configuration Management license](#)
[Device requirements for deployment and compliance tasks](#)

Creating a chassis deployment template from a chassis

You can create a chassis deployment template from a chassis that you have discovered along with the IOAs.

Before you create a chassis deployment template from a chassis, ensure that:


- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- The device from which you are creating a chassis template meets the requirements specified in [Device Requirements for Deployment and Compliance Tasks](#).
- The chassis and IOAs must be discovered by using WS-Man, REST, and SNMP protocols.

 **NOTE: The chassis template cannot be created if devices are discovered by using SNMP protocol only.**

To create a chassis deployment template from a chassis:

1. Click **Deployment** → **Deployment Portal**.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Create Template**.
 - In the **Templates** pane, right-click the **Chassis Template** and then click **Create Template**.

The **Create Template** window is displayed.

 **NOTE: If the deployment file share settings are not configured, a message stating that One or more settings require configuring for this action is displayed. If you click OK, the File Share Settings window is displayed. After you configure the file share settings, the Create Template Wizard is displayed.**

3. Type a **Name** for the template.
4. Select the device type (**Chassis** or **MX Chassis**), and perform one of the following:
 - Select a chassis device from the **All Applicable Devices** tree.

 **NOTE: Only the chassis with an Enterprise license and supported firmware version can be selected.**

- Search for a chassis device by using the **Search Devices** box.

5. Under **Execution Credentials**, type the chassis credentials and **IOA credentials(optional)**, and click **Finish**.

If the **IOA Credentials** are not provided, OpenManage Essentials creates only the chassis template and the IOA attributes are not captured in the template.

 **NOTE: If any mismatch of the credentials, the template creation task displays Warning state in the Task Execution History tab and the IOA attributes are not captured.**

6. In the task submission message, click **Ok**.

An import chassis template task is created in the **Tasks** tab in the right pane. You can view the status of the chassis deployment template in one of the following ways:

- View in the **Task Execution History** in the right pane.
- Double-click the task in **Task Execution History** to view the task execution details.

The chassis template is displayed in the **Chassis Templates** under **Templates** tab. Click the chassis template to view the chassis and IOAs attributes.

The IOAs are displayed as A1, A2, B1, B2, C1, C2, and selected by default for deployment. Click each IOA to view their attributes.

Managing chassis deployment templates

The chassis deployment templates contain various attributes of a chassis, or IOA (optional). Before you use the chassis template for deployment, you can:

- View the attributes of chassis deployment template.
- Deploy a chassis deployment template.
- Clone a chassis deployment template.
- Rename a chassis deployment template.
- Delete a chassis deployment template.
- Export the chassis deployment template.

 **NOTE: Compliance-related tasks are not supported for IOA attributes.**

Viewing and editing chassis deployment template attributes

1. Click **Deployment** → **Deployment Portal** → **Templates** pane.
2. Select either a sample chassis template or a chassis template that you created.
For MX7000 chassis, select an MX chassis template from the list.
The different groups of template attributes are displayed in the right pane
3. To edit an attribute, expand a group, and select the attribute that you want to edit, and then enter the new values for the attributes.
4. Click **Save**.
The template is updated with the changed attribute values.

 **NOTE: While editing an MX7000 chassis template attributes, you must select all the attributes available under a group, else the chassis template deployment task might fail.**

Exporting a chassis deployment template

The export option allows you to export the chassis infrastructure template into a .zip file. The .zip file contains the chassis template in .xml format and IOA template in .txt format.

To export a chassis template:

 **NOTE: Exporting a chassis deployment template exports all the attributes of the chassis template, including attributes that are not selected.**

1. Click **Deployment** → **Deployment Portal**.
2. In the **Templates** pane, right-click either a sample template or a template that you created, and then click **Export Template**.
The **Export Template** dialog box is displayed.
3. Click **Ok**.
4. Navigate to the location where you want to export the template, provide a file name, and then click **Save**.
Within the .zip file, the chassis template is saved in .xml format and IOA templates are saved in .txt format.

Cloning a chassis deployment template

You can clone a chassis deployment template to create a template that you can edit and deploy.

To clone a chassis deployment template:

1. Click **Deployment** → **Deployment Portal**
2. In the **Templates** pane, right-click a chassis template, and then click **Clone**.
The **Clone Configuration Template** window is displayed.
3. Type a name for the template, and click **Ok**.


The cloned template is displayed in the **Templates** pane under the chassis templates.

Deploying a chassis infrastructure template


The **Deploy Template** task allows you to deploy a chassis infrastructure template that includes chassis and IOA attributes, on a target device (chassis or IOA).

Before you begin deploying a chassis infrastructure template, ensure that:

- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- The target devices are added to the repurpose and bare-metal group. For more information, see [Adding Devices to the Repurpose and Bare Metal Devices Group](#).

 **NOTE:** From the **All Applicable Devices** tree, select only chassis to add to the repurpose and bare-metal group. Selecting the IOAs is not mandatory. If the IOA attributes are present in the template and the target chassis is in the bare-metal group, then the deployment happens on the IOAs also.

- You have created a chassis infrastructure template.
- The target devices meet the requirements that are specified in [Device Requirements for Deployment and Compliance Tasks](#).
- The Server Configuration Management license is installed on all target servers. For more information, see [OpenManage Essentials — Server Configuration Management License](#).

 **CAUTION:** Deploying a chassis infrastructure template on a device may result in potentially destructive changes to the device configuration including performance, connectivity, and ability to boot the device.

To deploy the chassis infrastructure template:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Deploy Template**.
 - In the **Templates** → **Chassis Templates** pane, right-click the chassis infrastructure template, and then click **Deploy**.
 - In the **Templates** → **MX Chassis Templates** pane, right-click the MX chassis template, and then click **Deploy**.

The **Deploy Template Wizard** is displayed.


3. On the **Name and Deploy Options** page:
 - a. Enter an appropriate name for the task.
 - b. Under **Deploy Target**, select **Bare Metal**.
 - c. Under **Select Deploy Options**, select **Deploy Template**.
 - d. Click **Next**.
4. On the **Select Template** page:
 - a. Click **Chassis Templates** or **MX Chassis Templates**.
 - b. Select the chassis infrastructure template that you want to deploy.

 **NOTE:** Only configuration templates that you have either created or cloned are available for selection.

- c. Click **Next**.
5. On the **Select Devices** page, select the target devices from the **All Applicable Devices** tree, and click **Next**.

 **NOTE:** Only devices of the same chassis model for which the chassis infrastructure template was created are available for selection.

6. On the **Edit Attributes** page:

 **NOTE:** OpenManage Essentials do not include any passwords from the source when the configuration template is created. If you want to set the passwords for the target devices, all password attributes must be edited in the configuration template before deployment. If you want to change the password, ensure to run the deployment task as a different user. If you are changing the password of the device through the deployment, ensure that you run the deployment task with a different user account.

- a. Click the **Template Attributes** tab to view the attribute groups with the list of attributes in a group.

 **NOTE:** The IOA fabrics that are selected for deployment of the chassis infrastructure template are displayed.

- b. Click the **Device Specific Attributes** tab to edit the attributes that are unique for the target device.


 **NOTE:** The **Device Specific Attributes** tab may or may not display attributes depending on the template that is selected for deployment.

- c. Click the attribute group name to view the list of attributes in a group.
- d. To assign a new Static IPv4 Address for the deployment, enter the Static IPv4 Address in the **Value** column of **IPv4Static 1 IPv4 Address** attribute.

 **NOTE:** Deploying the template with the changed Static IPv4 Address starts a new discovery task for the device. For more information about the task details, see [Task Status](#). The new Static IPv4 Address is added to the discovery range under **Manage** → **Discovery and Inventory** → **Discovery Ranges** → **All Ranges**.

 **NOTE:** If Static IPv4 Address is used in the deployment of a chassis template, then all the components in the chassis are rediscovered after the deployment task is completed.

- e. To edit the hostname of the IOA, enter the new hostname in the **Value** column of **IOA hostname** attribute.

 **NOTE:** The IOA hostname is changed to the new hostname after the discovery task is successful. For more information about the task details, see [Task Status](#). The IOAs with the new host names can be viewed under **Manage** → **Devices** → **All Devices**.

- f. Edit or select the values in the **Value** column depending on your preference.
g. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target device, clear the check box in the **Deploy** column.
h. Click **Save**.
i. Click **Next**.

7. On the **Options** page:

- a. Select **Continue on warnings** to continue with the deployment task even if the template is incompatible or shows warning messages.
b. Click **Next**.

8. On the **Set Schedule** page:

- a. Select either **Run now**, or click the calendar icon and select the date and time you want to run the task.
b. Under **Execution Credentials**, type the chassis credentials.
c. Under **IOA Credentials**, type the credentials that have the Administrator privileges on the IOA.

 **NOTE:** Ensure all the target IOAs have the same credentials. If the credentials mismatch on any of the IOA, then the deployment task fails for the particular IOA.

- d. Click **Next**.

9. On the **Summary** page, review the information that you have provided, and then click **Finish**.
The **Deploy Template** warning is displayed.

10. If you want to continue the deployment, click **Yes**.

The **Deploy Template** task is created and run based on the schedule you have selected. You can double-click the task in **Task Execution History** to view the task execution details.

Deploying IOA configuration template

The **Deploy Template** task allows you to deploy an IOA configuration template on a target device.

Before you begin deploying an IOA device configuration template, ensure that:

- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- The target devices are added to the **Repurpose and Bare Metal Devices** group or a compute pool. For more information, see [Adding Devices to the Repurpose and Bare Metal Devices Group](#).
- You have created a device configuration template from an IOA.
- The target devices meet the requirements specified in [Device Requirements for Deployment and Compliance Tasks](#).

 **NOTE:** Ensure that the IOA template that you want to import has not been edited after it was created. Editing an IOA template, compromises the integrity of the template. Therefore, deploying the edited IOA template results in a failure.

 **CAUTION:** Deploying a configuration template on a device may result in potentially destructive changes to the device configuration including performance, connectivity, and ability to boot the device.

To deploy the IOA configuration template:

1. Click **Deployment**.

The **Deployment Portal** is displayed.

2. Perform one of the following:

- In the **Common Tasks** pane, click **Deploy Template**.
- In the **Templates** pane, right-click the IOA template that you want to deploy, and click **Deploy**.
- In the **Compute Pools** pane, right-click a compute pool that has the target device, and then click **Deploy**.

The **Deploy Template Wizard** wizard is displayed.

3. On the **Name and Deploy Options** page:

- a. Type an appropriate name for the task.
- b. Under **Deploy Target**, select **Bare Metal**.
- c. Under **Select Deploy Options**, select **Deploy Template**.
- d. Click **Next**.

4. On the **Select Template** page:

- a. Select the IOA template that you want to deploy.

 **NOTE: Only configuration templates that you have either created or cloned are available for selection.**

- b. Click **Next**.

5. If applicable, on the **Select Virtual I/O Pool** page, click **Next**.

6. On the **Select Devices** page, select the target devices from the **All Applicable Devices** tree, and click **Next**.

 **NOTE: Only devices added to the Repurpose and Bare Metal Devices group are available for selection.**

7. On the **Edit Attributes** page:

- a. Select a device from the **Select Devices** list.
- b. Click the attribute group name to view the list of attributes in a group.
- c. Select the attributes that you want to deploy.
- d. Enter the values in the **Value** column based on your preference.
- e. Click **Save**.
- f. Click **Next**.

8. On the **Options** page:

- If you only want to verify if the device configuration template is deployed successfully, select **Perform pre-check only**.

 **NOTE: If the Perform pre-check only option is selected, by default the Continue on warnings option is disabled.**

- If you do not want to stop the deployment when the template is incompatible with the target devices, select **Continue on warnings**.

 **NOTE: When this option is selected, the warnings are ignored (if any) and the deployment task continues to run even if the device configuration template is incompatible.**

9. On the **Set Schedule** page:

- a. Select either **Run now**, or click the calendar icon and select the date and time you want to run the task.
- b. Under **Execution Credentials**, type the credentials that have the Administrator privileges on the IOA.
- c. Click **Next**.

10. On the Summary page, review the information that you have provided, and then click **Finish**.

The **Deploy Template** warning is displayed.

11. If you want to continue the deployment, click **Yes**.

The **Deploy Template** task is created and run based on the schedule you have selected. You can double-click the task in **Task Execution History** to view the task execution details.

IOA operational modes and the deployment task status

Table 62. IOA operational modes and the deployment task status

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/ Complete
PMUX	Standalone	Warning/ Complete
Virtual Link Trunk (VLT)	VLT	Complete
VLT	Non-VLT	Failed
Non-VLT	VLT	Failed


Deploying a network ISO image

The deploy template task allows you to boot a server to a network ISO image, after which you can deploy the ISO image on the server.

Before you begin deploying a network ISO image, ensure that:

- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- The target devices are added to the repurpose and bare-metal group. For more information, see [Adding Devices to the Repurpose and Bare Metal Devices Group](#).
- You have **Full Control** permission on the network share where the ISO image is available.
- The target devices meet the requirements specified in [Device Requirements for Deployment and Compliance Tasks](#).
- The Server Configuration Management license is installed on all target servers. For more information, see [OpenManage Essentials — Server Configuration Management License](#).

To deploy a network ISO image:

1. Click **Deployment**.
2. In the **Common Tasks** pane, click **Deploy Template**.
The **Deploy Template** wizard is displayed.
3. On the **Name and Deploy Options** page:
 - a. Type an appropriate name for the task.
 - b. Under **Select Deploy Options**, clear **Deploy Template** and select **Boot to Network ISO**.
 **NOTE:** If you want to deploy an operating system and a configuration template, you can select both the **Deploy Template** and **Boot to Network ISO** options. Separate tasks are created for each operation.
 - c. Click **Next**.
4. On the **Select ISO Location** page:
 - a. Under **ISO File Name**, type the name of the ISO image file.
 - b. Under **Share Location**, type the IP address and name of the network share.
 - c. Under **Share Credentials**, type the user name and password.
 - d. Click **Next**.
5. On the **Select Devices** page, select the target devices from the **Repurpose and Bare Metal Devices** tree, and click **Next**.

6. On the **Set Schedule** page:
 - a. Select either **Run now** or click the calendar icon and select the date and time you want to run the task.
 - b. Under **Execution Credentials**, type the credentials that have Administrator privileges on the iDRAC of the target servers.
 - c. Click **Next**.
7. On the Summary page, review the information that you have provided, and then click **Finish**.
8. If you want to continue the deployment, click **Yes**.

The **Boot to Network ISO** task is created and the task runs based on the schedule you have selected. You can double-click the task in **Task Execution History** to view the task execution details. After the target server boots to the network ISO image, you must launch the iDRAC virtual console and select the options for deploying the ISO image.

Related links

- [Deploy Template Wizard](#)
- [Device Configuration Setup Wizard](#)
- [Device requirements for deployment and compliance tasks](#)

Removing devices from the repurpose and bare-metal devices group

You can remove devices from the **Repurpose and Bare Metal Device** group after the device configuration deployment, network ISO image deployment, or auto deployment task is complete.

To remove devices from the **Repurpose and Bare Metal Devices** group:

1. Click **Deployment** → **Deployment Portal**.
2. In the **Repurpose and Bare Metal Devices** tab, select the devices you want to remove.
3. Perform one of the following:
 - Click **Remove Selected Devices**.
 - Right-click and select **Remove**.
4. On the confirmation dialog box, click **Yes**.

The devices are removed from the **Repurpose and Bare Metal Devices** tab in the right pane, and in the **Repurpose and Bare Metal Devices** group in the device tree.

Related link

- [Repurpose and Bare Metal Devices](#)

Auto deploying device configurations

The **Setup Auto Deployment** task enables you to deploy either a device configuration or network ISO image on target devices that you discover later. For example, if your company has ordered 500 systems that are expected to be delivered through the next two weeks, you can create the **Setup Auto Deployment** task. The **Setup Auto Deployment** task runs periodically and deploys the configuration after the devices are discovered.

When creating the task, you must import a .csv file that includes the Service Tags or node IDs of target devices on which you want to deploy the configuration. By default, the **Setup Auto Deployment** task is run every 60 minutes to identify if the target devices have been discovered. If a target device is discovered, the device configuration is automatically deployed to the target device. You can also modify the recurrence of the **Setup Auto Deployment** task based on your preference.

 **NOTE:** If you create auto deployment tasks in OpenManage Essentials version 2.0, 2.0.1, or 2.1 and then upgrade to version 2.2, 2.3, 2.4 or 2.5, the auto deployment tasks do not run successfully. In this scenario, Dell EMC recommends that you recreate the auto deployment tasks after upgrading OpenManage Essentials to version 2.2, 2.3, 2.4, or 2.5.

 **NOTE:** Auto Deployment feature is not applicable for IOA templates.

Related links

- [Configuring Auto Deployment Settings](#)
- [Setting up device configuration auto deployment—Bare-metal deployment](#)
- [Managing Auto Deployment Credentials](#)
- [Adding a Discovery Range for Auto Deployment](#)

Configuring Auto Deployment Settings

The **Auto Deployment Settings** allows you to perform the following:

- Enable or disable the device configuration auto deployment.
- Set the recurrence of the device configuration auto deployment task.

To configure the auto deployment settings:

1. Click **Settings** → **Deployment Settings**.
The **Deployment Settings** page is displayed.
2. Select or clear **Enable auto deployment for recently discovered devices** to enable or disable auto deployment of device configuration.
3. Edit the **Run auto deployment every xx Minutes** field based on your preference.
4. Click **Apply**.

Related link

- [Auto deploying device configurations](#)

Setting up device configuration auto deployment—Bare-metal deployment

The **Setup Auto Deployment** task enables you to deploy a configuration template, which includes a set of configuration attributes, to devices that you will discover at a later time. Deploying a device configuration template on the devices ensures that the devices are uniformly configured.

Before you create a device configuration auto deployment task, ensure that:

- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- The auto deployment setting is enabled and configured. For more information, see [Configuring Auto Deployment Settings](#).
- The Service Tag or node ID of each target device is available in a .csv file. The Service Tags or node IDs should be listed under the title 'ServiceTag', 'Service Tag', or 'Node ID' in the .csv file.



NOTE: On devices which have multiple compute nodes (such as the PowerEdge FM120x4), all of the compute nodes have the same Service Tag. Therefore, the node ID must be used to identify the specific compute node to use. In the .csv file, you must include the node IDs of the specific compute nodes that you want to auto deploy.

- You have either created a device configuration template or cloned a sample template.
- The target devices meet the requirements specified in [Device Requirements for Deployment and Compliance Tasks](#).
- The Server Configuration Management license is installed on all target servers. For more information, see [OpenManage Essentials — Server Configuration Management License](#).



CAUTION: Deploying a configuration template on a device may result in potentially destructive changes to the device configuration including performance, connectivity, and ability to boot the device.

To auto deploy the configuration template on devices that will be discovered at a later time:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Setup Auto Deployment**.
 - Click **Auto Deployment**, and then click **Add Devices**.

The **Setup Auto Deployment** wizard is displayed.

3. On the **Select Deploy Options** page:
 - a. Under **Deploy Target**, click **Bare Metal**.
 - b. If you want to auto deploy a configuration template and then boot the device to an operating system ISO image, you can select both the **Deploy Template** and **Boot to Network ISO** options. Separate tasks are created for each operation.
 - c. Click **Next**.
4. On the **Select Template** page:
 - a. Based on the target device type, click **Server Template** or **Chassis Template**.
 - b. Select the configuration template you want to deploy.


 **NOTE: Only configuration templates that you have either created or cloned are available for selection.**

- c. Click **Next**.
5. On the **Import Service Tags/Node IDs** page:
 - a. Click **Import**.
 - b. Browse and select the .csv file that includes the Service Tags or node IDs.

 **NOTE: You can only import valid Service Tags or node IDs that have not already been discovered.**

- c. Click **Open**.
The **Import Summary** is displayed.
 - d. Click **Ok**.
 - e. Click **Next**.


6. On the **Edit Attributes** page:

 **NOTE: OpenManage Essentials does not include any passwords from source when the configuration template is created. If you want to set the passwords for the target devices, all password attributes must be edited in the configuration template before deployment.**

- a. Click the **Template Attributes** tab.
 - b. Click the attribute group name to view the list of attributes in a group.
 - c. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target device, clear the check box in the **Deploy** column.
 - d. Edit or select the values in the **Value** column based on your preference.
The total number of attributes in the template and the number of attributes that you edit are displayed in the **Grouped by** bar.
 - e. Click the **Device Specific Attributes** tab to edit the attributes that are unique for the target device.

 **NOTE: The Device Specific Attributes tab may or may not display attributes based on the template selected for deployment.**

- f. Click the attribute group name to view the list of attributes in a group.
 - g. To assign a new Static IPv4 Address for the deployment, enter the Static IPv4 Address in the **Value** column of **IPv4Static 1 IPv4 Address** attribute.

 **NOTE: Deploying the template with the changed Static IPv4 Address initiates a new discovery task for the device. For more information on the task details, see [Task Status](#). The new Static IPv4 Address is added to the discovery range under **Manage** → **Discovery and Inventory** → **Discovery Ranges** → **All Ranges**.**

 **NOTE: If Static IPv4 Address is used in the deployment of a chassis template, then all the components in the chassis are rediscovered after the deployment task is completed.**

- h. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target device, clear the check box in the **Deploy** column.
 - i. Edit or select the values in the **Value** column based on your preference.

 **NOTE: You can also export the Device Specific Attributes for a specific device or for all devices as .csv file, edit the attributes, and import the attributes. To export or import the Device Specific Attributes, click **Import/Export**.**

- j. (For IOA VLAN configuration deployment only) Click the **IOA VLAN Attributes** tab to edit the IOA VLAN attributes for the selected template.
 - k. Select the **Deploy** check box for the attributes that you want to deploy.

- l. Type the values for the tagged VLANs and untagged VLAN.
 - m. Click **Save**.
 - n. Click **Next**.
7. On the **Execution Credentials** page:
 - a. On the **Credentials** section, click **Add New Credentials**.

 **NOTE: For server configuration deployment — provide the iDRAC Administrator credentials; For chassis configuration deployment — provide the CMC Administrator credentials.**


The **Add Credentials** window is displayed.

- b. Type the description, Administrator user name, and password required to run the task on the target devices.
 - c. If you want to set the credentials as the default credentials for all target devices, select **Default**, and then click **Finish**.
 - d. Repeat step a to step c until you have configured the credentials required for running the task on all target devices.
 - e. On the **Devices** section, set the **Execution Credentials** for each target device.
 - f. (Only for IOA VLAN configuration deployment) Under **IOA Credentials**, type the credentials that have Administrator privileges on the IOA.
 - g. Click **Next**.
8. On the **Summary** page, review the information that you have provided, and then click **Finish**.
The **Deploy Template** warning is displayed.
 9. If you want to continue creating the **Setup Auto Deployment** task, click **Yes**.

The Service Tags or Node IDs are displayed in the **Auto Deployment** tab until the devices are discovered and inventoried in OpenManage Essentials. The **Deploy Configuration to Undiscovered Devices** task runs periodically and verifies if the devices are discovered and inventoried in OpenManage Essentials.

 **NOTE: The Deploy Configuration to Undiscovered Devices runs based on the frequency configured in Settings → Deployment Settings.**

After the discovery and inventory of the devices is completed and a deploy task is created, the devices are moved to the repurpose and bare-metal devices group. You can double-click the tasks in **Task Execution History** to view the task execution details. If you do not want to deploy any other device configuration on the devices, you can remove the devices from the repurpose and bare-metal devices group.

 **NOTE: Devices in the Auto Deployment tab are moved to the repurpose and bare-metal devices group, even if the auto deployment task fails. If you want to deploy the configuration template on those devices, you must create a new deployment task.**

Related links

[Auto deploying device configurations](#)
[Setup Auto Deployment Wizard](#)
[Importing Device Specific Attributes](#)
[Exporting Device Specific Attributes](#)
[Server Configuration Management license](#)
[Device requirements for deployment and compliance tasks](#)
[Auto Deployment](#)

Managing Auto Deployment Credentials

The **Manage Auto Deployment Credentials** task enables you to configure and assign execution credentials for target devices that have been set up for auto deployment.

To manage auto deployment credentials:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. In the **Common Tasks** pane, click **Manage Auto Deployment Credentials**.
The **Manage Auto Deployment Credentials** window is displayed.
3. If you want to add new credentials that you want to assign to a target device, click **Add New Credentials**.



NOTE: For server configuration deployment — provide the iDRAC Administrator credentials; For chassis configuration deployment — provide the CMC Administrator credentials.

- a. In the **Add Credentials** window, type the description, user name, and password.
- b. If you want to set the credentials as the default credentials for all target devices, select **Default**, and then click **Finish**.

The credentials that you added are displayed in the **Credentials** section.

4. If you want to update an existing credential, click the update icon.
 - a. In the **Add Credentials** window, edit the description, user name, and password as required.
 - b. If you want to set the credentials as the default credentials for all new target devices, select **Default**, and then click **Finish**.
5. If you want to delete an existing credential, click the delete icon, and then click **Ok** in the **Confirmation Required** dialog box.

The credentials that you deleted are removed from the **Credentials** section.
6. If you want to assign credentials to a target device, in the **Devices** section, select the appropriate credentials under **Execution Credentials**.
7. Click **Finish**.

Related links

[Auto deploying device configurations](#)
[Manage Auto Deployment Credentials](#)

Adding a Discovery Range for Auto Deployment

You can create a discovery range for the auto deployment task through either the **Auto Deployment** tab or the **Discovery and Inventory** portal.

Before you can add a discovery range through the **Auto Deployment** tab, you must setup an auto deployment task.

To add a discovery range through the **Auto Deployment** tab:

1. Click **Deployment** → **Deployment Portal**.

The **Repurpose and Bare Metal Devices** tab is displayed in the right pane.
2. In the right pane, click the **Auto Deployment** tab, and then click **Add Discovery Range**.

The **Discover Devices** wizard is displayed.
3. Follow the instructions from step 2 to step 5 in [Creating a Discovery and Inventory Task](#) to create the discovery range.

The discovery range is created in the **Discovery and Inventory** portal.

Related links

[Auto deploying device configurations](#)
[Auto Deployment](#)

Removing Devices From an Auto Deployment Task

If you do not want to perform auto deployment on a particular devices, you can remove those devices from the auto deployment task.

To remove devices from an auto deployment task:

1. Click **Deployment** → **Deployment Portal**.

The **Repurpose and Bare Metal Devices** tab is displayed in the right pane.
2. On the right pane, click the **Auto Deployment** tab, and select the devices you want to remove.
3. Perform one of the following:
 - Click **Remove Selected Devices**.
 - Right-click and select **Delete**.
4. On the confirmation dialog box, click **Yes**.

The devices are removed from the **Auto Deployment** tab.

Related link

[Auto Deployment](#)

Importing Device Specific Attributes

You can also import the device specific attributes for deployment, if you already have a .csv file that includes the attributes. Before you begin, make sure that the .csv file that you want to import meets the requirements specified in [Import File Requirements](#). To import the attributes:

1. On the **Edit Attributes** page of the **Deployment Template Wizard** or **Setup Auto Deployment** wizard, click **Import/Export**. The **Import/Export Device Specific Attributes** window is displayed.
2. Click **Import**. The import confirmation dialog box is displayed.
3. Click **Yes**.
4. Navigate and select the .csv file, and click **Open**. The **Import Summary** dialog box displays the number of imported attributes.
5. Click **OK**.
6. In the **Import/Export Device Specific Attributes** window, click **Close**.



Related link

[Import File Requirements](#)

Import File Requirements

The following table describes the column titles and data to be included in the .csv file that is used for importing device specific attributes.

Table 63. Import File Requirements

Field	Description
Device Name	The name of the device. During import, the device name is used to match with the name of the device selected for deployment.
Service Tag	The Service Tag of the device. The Service Tag must be provided for auto deployment tasks. For the deployment task, the Service Tag is optional if the device name is provided.
Parent	The attribute's direct parent fully qualified descriptor (FQDD). The parent value is used to match during import.
Attribute	The raw name of the configuration attribute. The name is used to match during import.
Value	The value of the attribute.  NOTE: Empty values are also valid and will be imported. Secure values are exported in a masked format. All imported values are selected for deployment.
Possible Values	The list of allowable values.  NOTE: If you include a value that is not permitted or present in the list, the value is not imported.

Exporting Device Specific Attributes

You can also export the device specific attributes to a .csv file, edit the attributes, and then import the attributes. Exporting the attributes enables you to use an alternative method to edit the attributes. To export the attributes:



NOTE: If you want to export the device specific attributes for only a specific device, select the device in the **Edit Attributes** page.

1. On the **Edit Attributes** page of the **Deployment Template Wizard** or **Setup Auto Deployment** wizard, click **Import/Export**. The **Import/Export Device Specific Attributes** window is displayed.
2. Click either **Export Selected Device** or **Export All Devices** based on your preference. If you selected **Export All Devices**, a confirmation dialog box is displayed.
3. Click **Yes**.
4. Navigate to the location where you want to save the .csv file, and click **Save**.

Viewing the Deployment Tasks

To view the deployment tasks that have been created:

1. Click **Deployment** → **Deployment Portal**.
2. In the **Tasks** pane on the left, select a task type. The **Task** tab on the right pane displays the tasks that have been created.

Related link

[Tasks](#)

Managing the Virtual Input-Output Identities of a Server—Stateless Deployment

The I/O interfaces of a server, such as NICs or HBAs, have unique identity attributes that are assigned by the manufacturer of the interfaces. These unique identity attributes are collectively known as the I/O identity of a server. The I/O identities uniquely identify a server on a network and also determine how the server communicates with a network resource using a specific protocol. Using OpenManage Essentials, you can automatically generate and assign virtual identity attributes to the I/O interfaces of a server.

Servers deployed using a device configuration template that contains virtual I/O identities are known to be stateless. Stateless deployments allow you to create a server environment that is dynamic and flexible. For example, deploying a server with virtual I/O identities in a boot-from-SAN environment allows you to quickly perform the following:

- Replace a failing or failed server by moving the I/O identity of the server to another spare server.
- Deploy additional servers to increase the computing capability during high workload.

The **Deployment** portal allows you to perform the following tasks that are required to manage the virtual I/O identity of a server:

- Create virtual I/O pools
- Create compute pools
- Deploy a server
- Reclaim the virtual I/O identity of a server
- Replace a server

Overview of Stateless Deployment

The steps that you must perform to deploy a device configuration template with virtual I/O attributes on target devices are as follows:

1. **Create a device configuration template** — Use the **Create Template** task in the **Common Tasks** pane to create a device configuration template. You can choose to create the template from either a configuration file or a reference device.
2. **Edit the device configuration template** — Select the template from the **Templates** pane, and edit the desired configuration attributes displayed in the right pane.

3. **Create Virtual I/O Pool** — Use the **Create Virtual I/O Pool** task in the **Common Tasks** pane to create a pool of one or more virtual I/O identity types. The virtual I/O identity pool is used to assign virtual I/O identities to the target devices.
4. **Create Compute Pool** — Use the **Create Compute Pool** task in the **Common Tasks** pane to create a group of servers that you want to use for a specific purpose. You can associate a device configuration template and virtual I/O pool to the compute pool.
5. **Deploy the device configuration template on target devices** — Use the **Deploy Template** task in the **Common Tasks** pane to deploy the device configuration template and virtual I/O identities on the target devices.

Related links

[Getting started for device configuration deployment](#)
[Creating a device deployment template](#)
[Editing a device deployment template](#)
[Creating a Virtual Input-Output Pool](#)
[Creating a Compute Pool](#)
[Deploying a device configuration template—Stateless deployment](#)

Virtual Input-Output Pools

A virtual I/O pool is a collection of one or more virtual I/O identity types that are required for network communication. A virtual I/O pool can contain a combination of any of the following virtual I/O identity types:

- Ethernet identity which is defined by the Media Access Control (MAC) address. MAC addresses are required for Ethernet (LAN) communications.
- Fibre Channel (FC) identity which is defined by the World Wide Node Name (WWNN) and World Wide Port Name (WWPN). A WWNN identity is assigned to a node (device) in an FC fabric and may be shared by some or all ports of a device. A WWPN identity is assigned to each port in an FC fabric and is unique to each port. WWNN and WWPN identities are required to support boot-from-SAN and for data access using FC and Fibre Channel over Ethernet (FCoE) protocols.
- iSCSI identity which is defined by the iSCSI Qualified Name (IQN). IQN identities are required to support boot-from-SAN using the iSCSI protocol.

OpenManage Essentials utilizes the virtual I/O pools to automatically assign virtual I/O identities to the device configuration template that is used for deploying a server.



NOTE: A virtual I/O pool can be associated with one or more compute pools.

Related links

[Creating a Virtual Input-Output Pool](#)
[Editing a Virtual Input-Output Pool](#)
[Viewing the Definitions of a Virtual Input-Output Pool](#)
[Renaming a Virtual Input-Output Pool](#)
[Deleting a Virtual Input-Output Pool](#)

Creating a Virtual Input-Output Pool

You can create a virtual I/O pool that contains one or more virtual I/O identity types.
To create a pool of virtual I/O identity types:


1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. Perform one of the following:
 - On the left pane, under **Common Tasks**, click **Create Virtual I/O Pool**.
 - On the left pane, under **Virtual I/O Pools**, right-click **Virtual I/O Pools** → **Create Virtual I/O Pool**.The **Create Virtual I/O Pool** wizard is displayed.
3. On the **Name and Description** page, type a unique name for the virtual I/O pool and an appropriate description, and then click **Next**.

4. On the **Ethernet Identities** page, perform one of the following:


 **NOTE:** If you do not want to include MAC addresses in the virtual I/O pool, clear the **Include MAC addresses in this pool** option, and then click **Next**.

- a. To specify the start address and the number of identities, perform the following:

1. In the **Specify the start address** box, type the start address that you want to predefine in the MAC addresses that will be generated.

 **NOTE:** The input address range (start address + number of identities) is validated against the existing address ranges for overlap when you are creating or editing a virtual I/O pool. The number of identities requested cannot be guaranteed in case the requested address range is overlapping with an existing virtual I/O pool address range.

2. In the **Number of Identities** box, type the identity values that you want to define, and then click **Next**.

 **NOTE:** For Converged Network Adapter (CNA) cards, WWNN and WWPN identities are derived from virtual FIP MAC address. In these scenarios, though the identities are not generated from the Ethernet Identities pool, these derived identities are counted against the Ethernet Identities pool. Ensure that necessary buffer is added while defining the Ethernet Identities pool size when virtual pool is used for deployment on servers with CNA cards.

- b. If you want to import the MAC addresses from a .csv file, click **Import from file** and perform the following:

 **NOTE:** You can import up to 1000 identities using a .csv file. The .csv file must have a column titled **Name** or **Value**.

1. Click **Import**.
2. On the **Import Wizard**, click **Import**.
3. Browse and select the .csv file and click **Open**. The **Import Results** window is displayed.
4. Close the **Import Results** window and the **Import Wizard**, and then click **Next**.

	A
1	Value
2	F4-23-A5-32-70-E2
3	2B-40-04-6B-88-E6
4	01-CC-FE-0B-BC-0A
5	C9-81-33-D5-D3-65
6	B7-BC-3C-CF-27-91
7	27-1B-B5-CC-4D-26

Figure 23. Sample .csv file with MAC addresses


5. On the **FCoE Node Name Identities** page, perform one of the following:

 **NOTE:** It is not necessary to have a virtual I/O pool with FC attributes for deploying on a Converged Network Adapter (CNA) card because the FC attributes are automatically generated by OpenManage Essentials based on the virtual FIP MAC address.

 **NOTE:** If you do not want to include fibre channel WWNN identities in the virtual I/O pool, clear the **Include Fibre Channel WWNN Identities in the pool** option, and then click **Next**.

- a. To specify the start address for the WWNN identities and the number of identities to be generated, perform the following:

1. In the **Specify the start address** box, type the start address that you want to predefine in the WWNN identities that will be generated.

 **NOTE:** The input address range (start address + number of identities) is validated against the existing address ranges for overlap when you are creating or editing a virtual I/O pool. The number of identities requested cannot be guaranteed in case the requested address range is overlapping with an existing virtual I/O pool address range.

2. In the **Number of Identities** box, type the identity values that you want to define, and then click **Next**.

- b. If you want to import the WWNN identities from a .csv file, click **Import from file** and perform the following:

 **NOTE:** You can import up to 1000 identities using a .csv file. The .csv file must have a column titled **Name** or **Value**.

1. Click **Import**.
2. On the **Import Wizard**, click **Import**.
3. Browse and select the .csv file and click **Open**. The **Import Results** window is displayed.
4. Close the **Import Results** window and the **Import Wizard**, and then click **Next**.


	A
1	Value
2	50:06:0e:80:10:13:93:20
3	50:06:0e:80:10:13:93:21
4	50:06:0e:80:10:13:93:22
5	50:06:0e:80:10:13:93:23
6	50:06:0e:80:10:13:93:24

Figure 24. Sample .csv file with WWNN identities

6. On the **FCoE Port Name Identities** page, perform one of the following:

 **NOTE:** If you do not want to include fibre channel WWPN identities in the virtual I/O pool, clear the **Include Fibre Channel WWPN Identities in the pool** option, and then click **Next**.

- a. To specify the start address for the WWPN identities and the number of identities to be generated, perform the following:
 1. In the **Specify the start address** box, type the start address that you want to predefine in the WWPN identities that will be generated.

 **NOTE:** The input address range (start address + number of identities) is validated against the existing address ranges for overlap when you are creating or editing a virtual I/O pool. The number of identities requested cannot be guaranteed in case the requested address range is overlapping with an existing virtual I/O pool address range.
 2. In the **Number of Identities** box, type the identity values that you want to define, and then click **Next**.
- b. If you want to import the WWPN identities from a .csv file, click **Import from file** and perform the following:

 **NOTE:** You can import up to 1000 identities using a .csv file. The .csv file must have a column titled **Name** or **Value**.

1. Click **Import**.
2. On the **Import Wizard**, click **Import**.
3. Browse and select the .csv file and click **Open**. The **Import Results** window is displayed.
4. Close the **Import Results** window and the **Import Wizard**, and then click **Next**.

	A
1	Value
2	20:06:0e:AE:22:BE:99:20
3	20:06:0e:AE:22:BE:99:21
4	20:06:0e:AE:22:BE:99:22
5	20:06:0e:AE:22:BE:99:23
6	20:06:0e:AE:22:BE:99:24

Figure 25. Sample .csv file with WWPN identities

7. On the **iSCSI IQN Identities** page, perform one of the following:

 **NOTE:** If you do not want to include iSCSI IQN identities in the virtual I/O pool, clear the **Include IQN Identities in the pool** option, and then click **Next**.

- a. If you want to provide a prefix for the iSCSI IQN identities that will be generated, click **Specify a prefix to allocate from**, and type the IQN in the appropriate field.

 **NOTE:** The typical iSCSI IQN format is: *iqn.date.domainname-in-reverse:storage-identifier*. For example, iqn.2001-04.com.example:storage.disk2.sys1.xyz.

 **NOTE:** The iSCSI IQN identifier string can include the following special characters: hyphen, comma, colon, and period.

- b. If you want to import the iSCSI IQN identities from a .csv file, click **Import from file** and perform the following:

 **NOTE:** You can import up to 1000 identities using a .csv file. The .csv file must have a column titled **Name** or **Value**.

1. Click **Import**.
2. On the **Import Wizard**, click **Import**.
3. Browse and select the .csv file and click **Open**. The **Import Results** window is displayed.
4. Close the **Import Results** window and the **Import Wizard**, and then click **Next**.

	A
1	Value
2	iqn.1993-01.com.example:storage.tape1.sys1.01
3	iqn.1994-01.com.example:storage.tape1.sys1.01
4	iqn.1995-01.com.example:storage.tape1.sys1.01
5	iqn.1992-01.com.example:storage.tape1.sys1.01
6	iqn.1992-01.com.example:storage.tape1.sys1.02

Figure 26. Sample .csv file with iSCSI IQN identities

8. On the **Summary** page, review the definitions with the number of identities that you provided for the I/O identity types, and then click **Finish**.

The virtual I/O pool that you created is displayed under **Virtual I/O Pools** on the left pane.

Related links

[Virtual Input-Output Pools](#)

[Create Virtual Input-Output Pool Wizard](#)

Editing a Virtual Input-Output Pool

You can edit a virtual I/O pool to add ranges that you had not specified earlier, add a new I/O identity type, or delete identity type ranges that have not been assigned to any compute pool.

To edit the definitions of a virtual I/O pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. On the left pane, under **Virtual I/O Pools**, right-click a virtual I/O pool, and then click **Edit**.
The **Create Virtual I/O Pool Wizard** is displayed.
3. Make the required changes to the definitions on the appropriate pages of the wizard.
4. On the **Summary** page, click **Finish**.

The changes you made to the virtual I/O pool are saved.

Related links

[Virtual Input-Output Pools](#)

[Create Virtual Input-Output Pool Wizard](#)

Viewing the Definitions of a Virtual Input-Output Pool

To view the definitions of a virtual I/O pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. On the left pane, under **Virtual I/O Pools**, right-click a virtual I/O pool, and then click **View**.
The **Create Virtual I/O Pool Wizard** is displayed.

3. Click **Next** to view the various I/O identity definitions of the virtual I/O pool.

Related links

[Virtual Input-Output Pools](#)

[Create Virtual Input-Output Pool Wizard](#)

Renaming a Virtual Input-Output Pool

To rename a virtual I/O pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. On the left pane, under **Virtual I/O Pools**, right-click the virtual I/O pool that you want to rename, and then click **Rename**.
The **Rename Virtual I/O Pool** window is displayed.
3. Type a new name and then click **OK**.

The virtual I/O pool is renamed.

Related link

[Virtual Input-Output Pools](#)

Deleting a Virtual Input-Output Pool

You can delete a virtual I/O pool if the virtual I/O pool is not locked.

To delete a virtual I/O pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. On the left pane, under **Virtual I/O Pools**, right-click the virtual I/O pool that you want to delete, and then click **Delete**.
3. At the **Delete Confirmation** prompt, click **Yes**.

The virtual I/O pool is deleted.

Related link

[Virtual Input-Output Pools](#)

Viewing the Virtual Input-Output Identities Assigned or Deployed on a Device

Deployed I/O identities are identities from a virtual I/O pool that are deployed on target devices. Assigned I/O identities are identities from a virtual I/O pool that are assigned to target devices prior to deploying the devices. You can assign virtual I/O identities to target devices using the **Edit Attributes** → **Identity Attributes** tab of the **Deploy Template Wizard**.

To view the virtual I/O identities that are assigned or deployed on a device:

 **NOTE:** If you want to view all devices and their assigned or deployed virtual I/O identities, click **Reports** → **Server Configuration** → **Assigned Identity Attributes**.

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. Under **Virtual I/O Pools** on the left pane, select a virtual I/O pool.
The **Virtual I/O Pool Summary** page is displayed on the right pane.
3. On the **Virtual I/O Pool Summary** page, click the **Devices with Identities** tab.
Devices with assigned or deployed virtual I/O identities are displayed on a grid.
4. Perform one of the following:
 - Right-click a device on the grid, and then click **View Identities**.
 - Double-click a device on the grid.

The **Identity Assignments** window displays the virtual I/O identities that are either assigned or deployed on the device.

Compute Pools

A compute pool is a group of servers that you want to use for a specific purpose. Typically, the servers in a compute pool share the same hardware configurations and attributes. Based on your requirement, you can create compute pools for various purposes such as:

- Managing the workload
- Managing servers of a business unit
- Managing servers in a geographic region

Creating a compute pool allows you to quickly deploy a new server or replace an existing server in a production environment.





 **NOTE: A compute pool can be associated with only one virtual I/O pool and one device configuration template.**

Related links




[Creating a Compute Pool](#)
[Deploying a device configuration template—Stateless deployment](#)
[Unlocking a Compute Pool](#)
[Editing the Definitions of a Compute Pool](#)
[Viewing the Definitions of a Compute Pool](#)
[Removing a Server From a Compute Pool](#)
[Renaming a Compute Pool](#)
[Deleting a Compute Pool](#)

Creating a Compute Pool

You can create a compute pool to group a set of servers for a specific purpose. To create a compute pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. Perform one of the following:
 - On the left pane, under **Common Tasks**, click **Create Compute Pool**.
 - On the left pane, under **Compute Pools**, right-click **Repurpose and Bare Metal** → **Create Compute Pool**.The **Create Compute Pool Wizard** is displayed.
3. On the **Name and Description** page, type a unique name for the compute pool and an appropriate description, and then click **Next**.
4. On the **Select Template** page, perform the following:
 -  **NOTE: Selecting a template is optional. You can select a template at a later time, either by editing the compute pool or while deploying a server. If you do not want to select a template, ensure that the Select Template for the Compute Pool option is not selected, and then click Next.**
 -  **NOTE: Only templates that you have previously created from a server or cloned are available for selection.**
 -  **NOTE: Templates that are already associated with a compute pool are not available for selection.**
 -  **NOTE: The template you select must be imported from a PowerEdge server with the latest iDRAC firmware installed. The template must include persistence policy attributes that allow the deployed virtual I/O identities to be persistent across reboots.**
 - a. Select the **Select Template for the Compute Pool** option.
 - b. Select a template from the list and click **Next**.
5. On the **Select ISO Location** page, perform the following:

 **NOTE:** If you do not want to provide the ISO location details, ensure that the **Boot Compute Pool from Network ISO** option is not selected, and then click **Next**.

- a. Select the **Boot Compute Pool from Network ISO** option.
 - b. Type the ISO file name, IP address and name of the network share in the appropriate fields, and then click **Next**.
6. On the **Select Virtual I/O Pool** page, perform one of the following:
- If you want to provide the virtual I/O identity attributes manually while deploying the template, click **User defined I/O assignment**, and then click **Next**.
 - If you want OpenManage Essentials to automatically assign virtual I/O identities to the servers in the compute pool, click **Automatic I/O assignment**, select a virtual I/O pool from the list, and then click **Next**.
7. On the **Select Devices** page, select the target devices you want to include in the compute pool from the **All Applicable Devices** tree, and click **Next**.
-  **NOTE:** Only devices in the **Repurpose and Bare Metal** group that are not members of any other compute pools are available for selection.
-  **NOTE:** A device that is already included in a compute pool cannot be included in another compute pool.
-  **NOTE:** Only devices that you select to include in the compute pool are available for stateless deployment.
8. (Only if you selected a template in step 4) On the **Edit Attributes** page, select and update the attributes based on your requirement, and click **Next**.
9. On the **Summary** page, review your selections, and then click **Finish**.

The compute pool that you created is displayed under **Compute Pools** on the left pane.

Related links

[Compute Pools](#)
[Create Compute Pool Wizard](#)

Deploying a device configuration template—Stateless deployment

The **Deploy Template** task allows you to deploy a configuration template that includes a set of configuration attributes to specific devices. Deploying a device configuration template on the devices ensures that the devices are uniformly configured.

Before you begin deploying a device configuration template, ensure that:

- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- The target devices are added to the compute pool. For more information, see [Creating a Compute Pool](#) and [Editing a Compute Pool](#).
- You have either created or cloned a device configuration template.
- The target devices meet the requirements specified in [Device Requirements for Deployment and Compliance Tasks](#).
- The Server Configuration Management license is installed on all target servers. For more information, see [OpenManage Essentials — Server Configuration Management License](#).
- On servers with a Mellanox HBA adapter, make sure that the version of adapter firmware installed is 02.34.50.10 X08 or later.
- For IOA configuration deployment, the template must be created from a blade server.

 **NOTE:** For the list of HBA card types that support stateless deployment, see “Supported cards for I/O Identity Optimization” in the iDRAC User’s Guide at Dell.com/idracmanuals.


 **CAUTION:** Deploying a configuration template on a device may result in potentially destructive changes to the device configuration including performance, connectivity, and ability to boot the device.

To deploy a configuration template on devices:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Deploy Template**.
 - In the **Compute Pools** pane, right-click the compute pool that includes the devices that you want to deploy, and then click **Deploy**.

The **Deploy Template Wizard** wizard is displayed.

3. On the **Name and Deploy Options** page:
 - a. Type an appropriate name for the task.
 - b. Under **Deploy Target**, select **Compute Pool**.
 - c. Select a compute pool from the **Select a Compute Pool** list.
 - d. Under **Select Deploy Options**, select **Deploy Template**.
 - e. Click **Next**.
4. On the **Select Template** page, select a device configuration template and click **Next**.

 **NOTE:** Only device configuration templates that you have either created or cloned are available for selection. A template that is already assigned to a compute pool is not available for selection.

5. On the **Select Virtual I/O Pool** page, perform one of the following, and then click **Next**.
 - Select **User defined I/O assignment** if you want to manually provide virtual I/O identities for the devices.
 - Select **Automatic I/O assignment** and select a virtual I/O pool from the list to allow OpenManage Essentials to automatically assign virtual I/O identities to the devices.
6. On the **Select Devices** page, select one or more target devices from the compute pool tree, and then click **Next**.
7. On the **Edit Attributes** page:

 **NOTE:** OpenManage Essentials does not include any passwords from the source when the configuration template is created. If you want to set the passwords for the target devices, all password attributes must be edited in the configuration template before deployment.

 **NOTE:** If you selected User defined I/O assignment in step 5, you must edit the I/O attributes of the template and provide the appropriate values in the **Edit Attributes** → **Device Specific Attributes** tab.


 **NOTE:** The BIOS attributes list of the device configuration template contains the BIOS.Virtual instance with the following attributes: **EnableBootDevices** and **DisableBootDevices**. Devices that you want to boot from must be included in the **EnableBootDevices** list.

- a. Click the **Template Attributes** tab to edit the attributes of the device configuration template.
- b. Click the attribute group name to view the list of attributes in a group.
- c. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target devices, clear the check box in the **Deploy** column.
- d. Edit or select the values in the **Value** column based on your preference.

The total number of attributes in the template and the number of attributes that you edit are displayed on the **Grouped by** bar.
- e. Click **Save**.
- f. Click the **Device Specific Attributes** tab to edit the attributes that are unique for the target devices.

 **NOTE:** The **Device Specific Attributes** tab may or may not display attributes based on the template selected for deployment.


- g. Under **Select Devices**, select a device.
- h. Click the attribute group name to view the list of attributes in a group.
- i. To assign a new Static IPv4 Address for the deployment, enter the Static IPv4 Address in the **Value** column of **IPv4Static 1 IPv4 Address** attribute.

 **NOTE:** Deploying the template with the changed Static IPv4 Address initiates a new discovery task for the device. For more information on the task details, see [Task Status](#). The new Static IPv4 Address is added to the discovery range under **Manage** → **Discovery and Inventory** → **Discovery Ranges** → **All Ranges**.

- j. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target device, clear the check box in the **Deploy** column.
- k. Edit or select the values in the **Value** column based on your preference.
- l. Click **Save**.
- m. (For automatic virtual I/O assignment only) Click the **Identity Attributes** tab to assign the virtual I/O identities.

 **NOTE:** For FCoE WWPN, WWNN, and virtual FIP attributes, if you deselect an attribute, all the other related attributes are deselected automatically.

 **NOTE:** For Intel network adapters, a single iSCSI initiator name is generated and deployed on all ports. You cannot deploy the IQN identity to only one port. By default, the IQN identity is deployed to all ports.

 **NOTE:** The Status column displays an Error status if the selected virtual I/O pool either does not contain the virtual I/O attributes or does not have sufficient virtual I/O identities.

1. Optional: Click **Assign Identities** to assign virtual I/O identities from the virtual I/O pool.
2. On the **Results** prompt, click **OK**. The **Identity Assignments** tab is displayed.
- n. (For IOA VLAN configuration deployment only) Click the **IOA VLAN Attributes** tab to edit the IOA VLAN attributes for the selected template.
- o. Select the **Deploy** check box for the attributes that you want to deploy.
- p. Type the values for the tagged VLANs and untagged VLAN.
- q. Click **Save**.
- r. Click **Next**.
8. On the **Set Schedule** page:
 - a. Select either **Run now**, or click the calendar icon and select the date and time you want to run the task.
 - b. Under **Execution Credentials**, type the credentials of the iDRAC that have Administrator privileges.
 - c. (Only for IOA VLAN configuration deployment) Under **IOA Credentials**, type the credentials that have Administrator privileges on the IOA.
 - d. Click **Next**.
9. On the **Preview** page:
 - a. Optional: Click **Preview** to verify if the attributes of the device configuration template will be deployed successfully on the target devices.
 - b. Click **Next**.
10. On the **Summary** page, review the information that you have provided, and then click **Finish**.
The **Deploy Template** warning is displayed.
11. If you want to continue the deployment, click **Yes**.

The **Deploy Template** task is created and the task runs based on the schedule you have selected. You can double-click the task in **Task Execution History** to view the task execution details. After the deployment is completed successfully, the template deployed


icon  and the text, **Deployed**, are displayed along with the device name in the compute pool.

 **NOTE:** On stateless deployment for FCoE protocol, the first octet for WWNN will be 20:00 and the first octet for the WWPN will be 20:01. The remaining octets will be the same as the virtual FIP MAC address.

Related links

[Server Configuration Management license](#)
[Device requirements for deployment and compliance tasks](#)
[Compute Pools](#)
[Automatic Locking of a Compute Pool](#)

Automatic Locking of a Compute Pool

After the first successful deployment of any server in a compute pool, the compute pool is automatically locked. When a compute pool is locked, the associated device configuration template and the virtual I/O pool are also locked. A lock icon  is displayed in the user interface to indicate that the resource is locked. Locking of the compute pool ensures that all servers in the pool utilize the same device configuration template and virtual I/O pool. You can only perform the following on a locked compute pool:

- View the definitions of the compute pool
- Add or remove servers from the compute pool
- Deploy servers that are members of the compute pool

 **NOTE:** If you want to use a locked device configuration template for other purposes, you can clone and use the device configuration template.

Unlocking a Compute Pool

You can unlock a compute pool if you want to update the compute pool after the compute pool is deployed and locked. For example, after unlocking a compute pool, you can edit the device configuration template, and then redeploy the servers in the compute pool. To unlock a compute pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. On the left pane, under **Compute Pools**, right-click the compute pool that you want to unlock, and then click **Unlock**.
3. At the confirmation prompt, click **Yes**.

The compute pool is unlocked. However, the servers in the compute pool that were already deployed remain in the deployed state. Unlocking the compute pool also unlocks the associated device configuration template and virtual I/O pool.

Related links

[Compute Pools](#)

[Automatic Locking of a Compute Pool](#)

Editing the Definitions of a Compute Pool

The definitions of a compute pool that you can edit depend on whether the compute pool is locked or unlocked. After any server in a compute pool is successfully deployed, the compute pool is automatically locked. In a locked compute pool, you can only add and deploy servers.

To edit the definitions of a compute pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. On the left pane, under **Compute Pools**, right-click a compute pool, and then click **Edit**.
The **Create Compute Pool Wizard** is displayed.
3. Make the required changes to the definitions on the appropriate pages of the wizard.
4. On the **Summary** page, review the information, and then click **Finish**.

The changes you made to the compute pool are saved.

Related links

[Compute Pools](#)

[Create Compute Pool Wizard](#)

Viewing the Definitions of a Compute Pool

To view the definitions of a compute pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. On the left pane, under **Compute Pools**, right-click a compute pool, and then click **View**.
The **Create Compute Pool Wizard** is displayed.
3. Click **Next** to view the various definitions of the compute pool.

Related links

[Compute Pools](#)

[Create Compute Pool Wizard](#)

Removing a Server From a Compute Pool

You can remove a server from a compute pool based on your requirement. For example, you can remove a server from a compute pool for the purpose of moving the server to another compute pool or for deploying the server without virtual I/O identities. To remove a server from a compute pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. On the left pane, under **Compute Pools**, right-click the server that you want to remove from the compute pool, and then click **Remove from Pool**.
3. At the confirmation prompt, click **Yes**.

The server is removed from the compute pool and is moved to the **Repurpose and Bare Metal Devices** group.

Related link

[Compute Pools](#)

Renaming a Compute Pool

To rename a compute pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. On the left pane, under **Compute Pools**, right-click the compute pool that you want to rename, and then click **Rename**.
The **Rename Compute Pool** window is displayed.
3. Type a new name and then click **OK**.

The compute pool is renamed.

Related link

[Compute Pools](#)

Deleting a Compute Pool

To delete a compute pool:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. On the left pane, under **Compute Pools**, right-click the compute pool that you want to delete, and then click **Delete**.
3. At the **Delete Confirmation** prompt, click **Yes**.

The compute pool is deleted and all servers from the pool are returned to the **Repurpose and Bare Metal** group. The virtual I/O pool and the device configuration template that was associated with the compute pool are unlocked. However, virtual I/O identities that were either assigned or deployed are retained by the servers.



NOTE: Even if the compute pool is deleted, the servers that were part of the compute pool remain in the deployed state.

Related link

[Compute Pools](#)


Replacing a Server

The replace server task allows you to quickly replace a production server with another server from within the same compute pool. For example, you can use the replace server task to quickly replace a failing or failed server with another spare server. When the replace server task runs, the attributes of a device configuration template and the virtual I/O identities of the source server are migrated to the target server.

Before you begin the replace server task, ensure that:

- The compute pool contains a minimum of two servers, one or both of the servers in a deployed state.
- The source server is deployed within the same compute pool.
- The target server is within the same compute pool as the source server.

To replace a server:

 **CAUTION:** The replace server task may result in potentially destructive changes to the device configuration including performance, connectivity, ability to boot the device, and/or data loss.

1. Click **Deployment**.

The **Deployment Portal** is displayed.


2. Perform one of the following:

- In the **Common Tasks** pane, click **Replace Server**.
- In the **Compute Pools** pane, right-click the compute pool that includes the server you want to replace, and then click **Replace Server**.

The **Replace Server Wizard** wizard is displayed.

3. On the **Name** page, type an appropriate name for the task, and then click **Next**.

4. On the **Source and Target** page:

 **NOTE:** The target servers are displayed only after you select the source server. The servers displayed in the **Select Target** section also include servers that are already in a deployed state.

- Under **Select Source**, select the source server.
- Under **Select Target**, select the target server.
- Click **Next**.

5. On the **Review Source Attributes** page, review the template attributes, IOA VLAN attributes (if applicable), device specific attributes, and virtual I/O identity assignments, and then click **Next**.

6. On the **Options** page, select any of the following options based on your preference:

- **Remove source from compute pool** — Select to move the source server from the compute pool to the **Repurpose and Bare Metal Devices** group after the server is replaced.
- **Deploy to target even if virtual identities cannot be reclaimed from the source** — Select to reclaim the virtual I/O identities of the source server, even if the source server is unreachable.

7. Click **Next**.


8. On the **Credentials** page, type the iDRAC user name and password of the source server and target server in the appropriate fields, and then click **Next**.


9. On the **Summary** page, review the selections you have made, and then click **Finish**.


The **Replace Server** warning is displayed.

10. If you want to continue the replacement, click **Yes**.

The replace server task is created and the task runs immediately. You can double-click the task in **Task Execution History** to view

the task execution details. After the deployment is completed successfully, the template deployed icon  and the text, **Deployed**, are displayed along with the device name in the compute pool.

 **NOTE:** When a server is replaced, all selected attributes of the device configuration template (including device-specific identity attributes for workload movement) are deployed on the target server. If you try to redeploy the device configuration template after replacing the server, the device-specific attributes are not populated automatically in the **Deploy Template** wizard. Therefore, if required, you must manually enter the device-specific attributes in the **Edit Template** page of the **Deploy Template** wizard.


 **NOTE:** When the replace server task runs, the pie chart in the **Device Compliance** portal displays the source server as two devices — one as **Not Compliant** or **Compliant** and another as **Not Inventoried**. After the server replacement task is completed, the pie chart displays the correct compliance status for the source server.

Reclaiming Deployed Virtual Input-Output Identities of a Server

The reclaim identities task allows you to reclaim all deployed virtual I/O identities from a server. Before you begin the reclaim identities task, ensure that:

- The server has been deployed from a compute pool.
- The server has been assigned virtual I/O identities using OpenManage Essentials.

To reclaim the deployed virtual I/O identities of a server:

 **CAUTION: The reclaim identities task may impact one or more network settings of the server and may result in loss of connectivity to the server.**

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Reclaim Identities**.
 - In the **Compute Pools** pane, right-click the compute pool that includes the server you want to replace, and then click **Reclaim Identities**.
 - In the **Virtual I/O Pools** pane, click a virtual I/O pool. On the right-side pane, click the **Devices with Identities** tab. Right-click a device and then click **Reclaim Deployed Virtual Identities**.

The **Reclaim Identities Wizard** wizard is displayed.
3. On the **Name** page, type an appropriate name for the task, and then click **Next**.
4. On the **Select Devices** page, click **Next**.
5. On the **Identity Assignments** page, review the virtual I/O identity attributes, and then click **Next**.
6. On the **Options** page, select any of the following options based on your preference:
 - **Remove source from compute pool** — Select to move the servers from the compute pool to the **Repurpose and Bare Metal Devices** group after reclaiming the virtual I/O identities.
 - **Force reclaim action even if target cannot be contacted** — Select to reclaim the virtual I/O identities of the server, even if source server is unreachable.
7. Click **Next**.
8. On the **Credentials** page, type the user name and password of the iDRAC in the appropriate fields, and then click **Next**.
9. On the **Summary** page, review the selections you have made, and then click **Finish**.
The **Reclaim Identities** warning message is displayed.
10. If you want to continue reclaiming the virtual I/O identities of the server, click **Yes**.

The reclaim identities task is created and the task runs immediately. You can double-click the task in **Task Execution History** to view the task execution details.

Reclaiming Assigned Virtual Input-Output Identities

You can also reclaim the assigned virtual I/O identities from a device based on your preference. To reclaim the assigned virtual I/O identities:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. Under **Virtual I/O Pools** on the left pane, select a virtual I/O pool.
The **Virtual I/O Pool Summary** page is displayed on the right pane.
3. On the **Virtual I/O Pool Summary** page, click the **Devices with Identities** tab.
Devices with assigned or deployed virtual I/O identities are displayed on a grid.
4. Right-click a device on the grid and then click **Reclaim Assigned Identities**.
The reclaim assigned identities warning message is displayed.

5. If you want to continue reclaiming the assigned virtual I/O identities of the device, click **Yes**.

The reclaimed virtual I/O identities are returned to the virtual I/O pool.

Setting up device configuration auto deployment—Stateless deployment

The **Setup Auto Deployment** task enables you to deploy a configuration template, which includes a set of configuration attributes, to devices that you will discover at a later time. Deploying a device configuration template on the devices ensures that the devices are uniformly configured.

Before you create a device configuration auto deployment task, ensure that:

- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- The auto deployment setting is enabled and configured. For more information, see [Configuring Auto Deployment Settings](#).
- The Service Tag or node ID of each target device is available in a .csv file. The Service Tags or node IDs should be listed under the title 'ServiceTag', 'Service Tag', or 'Node ID' in the .csv file.



NOTE: On devices which have multiple compute nodes (such as the PowerEdge FM120x4), all of the compute nodes have the same Service Tag. Therefore, the node ID must be used to identify the specific compute node to use. In the .csv file, you must include the node IDs of the specific compute nodes that you want to auto deploy.

- You have either created a device configuration template or cloned a sample template.
- You have already created a compute pool. For more information, see [Creating a Compute Pool](#).
- The target devices meet the requirements specified in [Device Requirements for Deployment and Compliance Tasks](#).
- The Server Configuration Management license is installed on all target servers. For more information, see [OpenManage Essentials — Server Configuration Management License](#).
- On servers with a Mellanox HBA adapter, make sure that the version of adapter firmware installed is 02.34.50.10 X08 or later.
- For IOA configuration deployment, the template must be created from a blade server.



CAUTION: Deploying a configuration template on a device may result in potentially destructive changes to the device configuration including performance, connectivity, and ability to boot the device.

To auto deploy the configuration template on devices that will be discovered at a later time:

1. Click **Deployment**.
The **Deployment Portal** is displayed.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Setup Auto Deployment**.
 - Click **Auto Deployment**, and then click **Add Devices**.The **Setup Auto Deployment** wizard is displayed.
3. On the **Select Deploy Options** page:
 - a. Under **Deploy Target**, select a compute pool from the **Select a Compute Pool** list.
 - b. Under **Select Deploy Options**, select **Deploy Template**.
 - c. Click **Next**.

4. On the **Select Template** page, select a configuration template, and then click **Next**.



NOTE: Only configuration templates that you have either created or cloned are available for selection.

5. On the **Select Virtual I/O Pool** page, perform one of the following, and then click **Next**.
 - Select **User defined I/O assignment** if you want to edit the attributes of the template to provide virtual I/O identities for the devices.
 - Select **Automatic I/O assignment** and select a virtual I/O pool from the list to allow OpenManage Essentials to automatically assign virtual I/O identities to the devices.
6. On the **Select Virtual I/O Pool** page,
7. On the **Import Service Tags/Node IDs** page:
 - a. Click **Import**.
 - b. Browse and select the .csv file that includes the Service Tags or node IDs.



NOTE: You can only import valid Service Tags or node IDs that have not already been discovered.

- c. Click **Open**.
The **Import Summary** is displayed.
- d. Click **Ok**.
- e. Click **Next**.

8. On the **Edit Attributes** page:



NOTE: OpenManage Essentials does not include any passwords from source when the configuration template is created. If you want to set the passwords for the target devices, all password attributes must be edited in the configuration template before deployment.

- a. Click the **Template Attributes** tab.
- b. Click the attribute group name to view the list of attributes in a group.
- c. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target device, clear the check box in the **Deploy** column.
- d. Edit or select the values in the **Value** column based on your preference.
The total number of attributes in the template and the number of attributes that you edit are displayed in the **Grouped by** bar.
- e. If you made any changes, click **Save**.
- f. Click the **Device Specific Attributes** tab to edit the attributes that are unique for the target device.



NOTE: The **Device Specific Attributes** tab may or may not display attributes based on the template selected for deployment.

- g. Click the attribute group name to view the list of attributes in a group.
- h. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target device, clear the check box in the **Deploy** column.
- i. Edit or select the values in the **Value** column based on your preference.



NOTE: You can also export the **Device Specific Attributes** for a specific device or for all devices as .csv file, edit the attributes, and import the attributes. To export or import the **Device Specific Attributes**, click **Import/Export**.

- j. Click the **Identity Attributes** tab to review the virtual I/O attributes.
- k. If you do not want to deploy a particular attribute in the template and want to retain the current attribute value on the target device, clear the check box in the **Deploy** column.
- l. If you made any changes, click **Save**.
- m. (For IOA VLAN configuration deployment only) Click the **IOA VLAN Attributes** tab to edit the IOA VLAN attributes that are unique for the target device.
- n. Select the **Deploy** check box for the attributes that you want to deploy.
- o. Type the values for the tagged VLANs and untagged VLAN.
- p. Click **Save**.
- q. Click **Next**.

9. On the **Execution Credentials** page:

- a. On the **Credentials** section, click **Add New Credentials**.
The **Add Credentials** window is displayed.
- b. Type the description, Administrator user name, and password required to run the task on the target devices.
- c. If you want to set the credentials as the default credentials for all target devices, select **Default**, and then click **Finish**.
- d. Repeat step a to step c until you have configured the credentials required for running the task on all target devices.
- e. On the **Devices** section, set the **Execution Credentials** for each target device.
- f. (Only for IOA VLAN configuration deployment) Under **IOA Credentials**, type the credentials that have Administrator privileges on the IOA.
- g. Click **Next**.


10. On the **Summary** page, review the information that you have provided, and then click **Finish**.

The **Deploy Template** warning is displayed.

11. If you want to continue creating the **Setup Auto Deployment** task, click **Yes**.

The Service Tags or Node IDs are displayed in the **Auto Deployment** tab until the devices are discovered and inventoried in OpenManage Essentials. The **Deploy Configuration to Undiscovered Devices** task runs periodically and verifies if the devices are discovered and inventoried in OpenManage Essentials.

 **NOTE: The Deploy Configuration to Undiscovered Devices runs based on the frequency configured in Settings → Deployment Settings.**

After the discovery and inventory of the devices is completed and a deploy task is created, the devices are moved to appropriate compute pool. You can double-click the tasks in **Task Execution History** to view the task execution details. After the deployment is completed successfully, the template deployed icon  and the text, **Deployed**, are displayed along with the device name in the compute pool.

Related link

[Server Configuration Management license](#)

Viewing device profiles

The profile of a device contains a list of last deployed attributes of the device configuration template, including the device-specific and virtual I/O identity attributes.

To view a device profile with last deployed attributes:

Perform one of the following:

- On the **Devices** portal, select the deployed device from the device tree. On the right-pane, click **Configuration** → **Profile**.
- On the **Deployment** portal, select the deployed device from the **Compute Pool** section. On the right-pane, click **Profile**.

The last deployed attributes are displayed within the **Template Attributes**, **Device-Specific Attributes**, and **Virtual Identities** tabs.

 **NOTE: Only attributes that you selected in the device configuration template for the deployment are displayed in the Profile tab.**

Known limitations for stateless deployment

The following are the known limitations for deploying virtual I/O identities on target servers:

- On Broadcom network adapters, OpenManage Essentials does not support boot from ISO for installing the operating system on a SAN along with the virtual I/O identity deployment. However, if an operating system is already installed on the SAN, after deployment of virtual I/O identities, the server can boot from the SAN.
- For PowerEdge FC430, FC630, and FC830 sleds, the PCIe cards (FC and iSCSI) in the shared PCIe slots of the PowerEdge FX2s chassis are supported for stateless deployment. However, if the PCIe cards are mapped, replacement can be performed only to an exactly similar sled in the same slot with the same PCIe mapping in another chassis. If the PCIe cards are not mapped, replacement can be performed on any similar sled.
- For performing stateless deployment on blade servers, the FlexAddress mode must be disabled on the blade server to prevent the host chassis from assigning I/O identity attributes. Even if the FlexAddress mode is enabled, OpenManage Essentials overrides the FlexAddress mode.
- While performing a stateless deployment on a server with a QLogic Converged Network Adapter, OpenManage Essentials generates different attribute values for the virtual MAC (vMAC) and virtual FIP (vFIP) MAC attributes. However, only the value of the vMAC attribute is deployed for both the vMAC and vFIP MAC attributes. If you create a zone for SAN boot before the deployment, ensure that the zone is created based on the vMAC address generating virtual WWPN (vWWPN) and virtual WWNN (vWWNN). For example, 20:00:vMAC for vWWNN and 20:01:vMAC for vWWPN.
- Intel NIC cards do not support unique iSCSI initiator name for each port. OpenManage Essentials deploys the same IQN value for all ports in the Intel NIC card.

Additional information

The following technical white papers and files available at delltechcenter.com provide additional information about the device configuration template, attributes, and workflows:

- *Server Cloning with Server Configuration Profiles*
- *Server Configuration XML File*
- *Configuration XML Workflows*
- *Configuration XML Workflow Scripts*
- *XML Configuration File Examples*

You can also find detailed information about bare-metal and stateless deployments by using OpenManage Essentials in the server deployment technical white paper available at DellTechCenter.com/OME.

Deployment—Reference

You can access the following from the **Deployment** → **Deployment Portal** page:




- Deploy Device Configuration Portal
 - Getting Started for Deployment—Displays the information required to setup, use, and get started with the device configuration deployment features.
 - Deployment Portal—Displays the default view of the **Deployment Portal**.
- Common Tasks—Displays the deployment setup tasks and other tasks that you can create.
 - Create Template
 - Create Virtual I/O Pool
 - Create Compute Pool
 - Deploy Template
 - Setup Auto Deployment
 - Manage Auto Deployment Credentials
 - File Share Settings
 - Replace Server
 - Reclaim identities
- Templates—Displays the sample device configuration templates and templates that you have created or cloned.
 - Server Templates
 - Sample - iDRAC SNMP Management Settings
 - Sample - iDRAC Auto Update Settings
 - Sample - Enable Broadcom Partitioning
 - Sample - BIOS Setup System Password
 - Sample - iDRAC static IP address
 - Sample - iDRAC System Location
 - Sample - iDRAC Thermal Alert Monitor
 - Sample - iDRAC Timezone NTP
 - Sample - Configure iDRAC Users
 - Sample - iDRAC Initialized Virtual Disk
 - Sample - Set Virtual Disk As Boot
 - Sample - Delete BIOS System Setup Password
 - Sample - Enable PXE Boot
 - Sample - One Time BIOS Boot Device
 - Sample - One Time HD Boot Device
 - Sample - One Time UEFI Boot Device
 - Sample - Set BIOS Boot Order
 - Sample - Set HD Boot Order





- Sample - iDRAC Set Power Cap
- Sample - Set UEFI Boot Order
- Sample - Set SNMP Email Alerts
- Chassis Templates
 - Sample - FX2 Chassis
 - Sample - VRTX Chassis
 - Sample - M1000e Chassis
- MX Chassis Templates
 - Sample - MX7000 Chassis
- IOA Templates
- Compute Pools—Displays the devices you have added to the **Repurpose and Bare Metal** group and the compute pools that you have created.
- Virtual I/O Pools—Displays the virtual I/O identity pools that you have created.
- Tasks—Displays the tasks of the selected category in the **Tasks** tab in the right pane.
- Configuration Tasks
 - MX Chassis Configuration Deployment—Displays the device configuration deployment tasks that you have created for MX7000 Chassis.
 - MX Chassis Configuration Import—Displays the **Create Template** tasks you have created for MX7000 chassis.
 - IOA Configuration Pre-Check—Displays the device configuration pre-check tasks that you have created for IOAs.
 - IOA Configuration Deployment—Displays the device configuration deployment tasks that you have created for IOAs.
 - IOA Configuration Import—Displays the **Create Template** tasks that you have created for IOAs.
 - Replace Server—Displays the history of the replaced servers.
 - Reclaim Identities—Displays the history of the reclaimed virtual I/O identities.
 - Device Configuration Preview—Displays the history of the device configuration deployment preview.
 - Deploy to Undiscovered Devices—Displays the **Auto Deployment Tasks** you have created.
 - Device Configuration Image Deploy—Displays the **Boot to Network ISO** tasks that you have created.
 - Chassis Configuration Deployment—Displays the device configuration deployment tasks you have created for chassis.
 - Chassis Configuration Import—Displays the **Create Template** tasks you have created for chassis.
 - Device Configuration Deployment—Displays the device configuration deployment tasks you have created for servers.
 - Device Configuration Import—Displays the **Create Template** tasks you have created for servers.

 **NOTE:** For information on the sample device configuration templates, see the iDRAC documentation at [Dell.com/support](https://dell.com/support).

Icons and descriptions

Table 64. Icons and descriptions

Icon	Description
	Read-only device configuration template. Read-only templates must be cloned before you can use it for deployment or configuration compliance tasks.
	Created, imported, or cloned device configuration template.
	Device configuration template is successfully deployed on the target device.

Icon	Description
	Virtual I/O pool.
	Compute pool.
	A locked resource.
	Read-only but deployable device configuration template.

Related links

[Repurpose and Bare Metal Devices](#)
[Auto Deployment](#)
[Tasks](#)
[Task Execution History](#)
[Device Configuration Template Details](#)
[IOA VLAN Attributes](#)
[Device Configuration Setup Wizard](#)
[Create Template Wizard](#)
[Deploy Template Wizard](#)
[Setup Auto Deployment Wizard](#)
[Manage Auto Deployment Credentials](#)

Repurpose and Bare Metal Devices

The **Repurpose and Bare Metal Devices** tab displays the devices that you have added to the **Repurpose and Bare Metal Devices** group and the compute pools that you have created. This tab also displays the last deploy result and last template deployed to the devices.

 **NOTE:** The **Repurpose and Bare Metal Devices** tab only displays devices that are not included in any compute pool.

The fields displayed in the **Repurpose and Bare Metal Devices** tab are described in the following table.

Table 65. Repurpose and Bare Metal Devices

Field	Description
Last Deploy Result	Displays the result of the last deployment task.
Device Name	Displays the device name.
Service Tag	Displays the unique identifier assigned to the system.
Model	Displays the model name of the system. For example, PowerEdge R710.
Last Template Deployed	Displays the latest template deployed.
End Time	Displays the date and time when the latest template was deployed.
Modify Devices	Displays the All Applicable Devices tree view. Select or clear devices to add or remove the devices from the Repurpose and Bare Metal Devices group.
Remove Selected Devices	Removes the selected devices from the Repurpose and Bare Metal Devices group.

Related links

[Removing devices from the repurpose and bare-metal devices group](#)
[Adding devices to repurpose and bare-metal devices group](#)

Auto Deployment

The **Auto Deployment** tab displays the target devices that you have selected for the auto deployment tasks.

The fields displayed in the **Auto Deployment** tab are described in the following table.

Table 66. Auto Deployment

Field	Description
Service tag or Node ID	Displays the unique identifier assigned to the system.
Template to Deploy	Displays the template selected for deployment on the device.
Compute Pool	Displays the name of the compute pool to which the device belongs.
Virtual IO Pool	Displays the name of the virtual IO pool to which the device belongs.
Boot to Network ISO	Displays if you have selected to boot the server to a network ISO image.
Configure VLANs on IOAs	Displays if you have selected to configure the VLANs on the IOAs.
Created On	Displays the date the auto deployment task was created.
Created By	Displays the name of the user who created the task.
Add Discovery Range	Displays the Discovery Range Configuration wizard that enables you to add a discovery range.
Add Devices	Displays the Setup Auto Deployment wizard.
Remove Selected Devices	Removes the selected devices from the associated Setup Auto Deployment tasks.

Related links

[Adding a Discovery Range for Auto Deployment](#)
[Removing Devices From an Auto Deployment Task](#)
[Setting up device configuration auto deployment—Bare-metal deployment](#)

Tasks

The fields displayed in the **Tasks** tab of the **Deployment** portal are described in the following table.

Table 67. Tasks

Field	Description
Schedule	Displays if the task schedule is active or inactive.
Task Name	Displays the name of the task.
Type	Displays the type of the task.
Description	Displays a brief description about the task.
Updated On	Displays the date and time the task was updated.
Updated By	Displays the name of the user who updated the task.
Created On	Displays the date and time the task was created.

Field	Description
Created By	Displays the name of the user who created the task.

Related link






[Viewing the Deployment Tasks](#)

Task Execution History

The **Task Execution History** tab displays the status of tasks.

The fields displayed in the **Task Execution History** tab are described in the following table.

Table 68. Task Execution History

Field	Description
Status	Displays an icon representing the task status:  — Running or pending  — Complete  — Stopped  — Failed  — Warning
Task Name	Displays the name of the task.
Start Time	Displays the start time of the task.
% Completed	Displays the progress information of the task.
Task State	Displays the state of the task: <ul style="list-style-type: none"> Running Complete Stopped Failed Warning
End Time	Displays the end time of the task.
Executed by User	Displays the name of the user who executed the task.

Device Configuration Template Details

The fields displayed in the **Attributes** pane of the **Deployment Portal** are described in the following table.

Table 69. Device Configuration Template Details

Field	Description
Undo	Click to undo the changes made to the configuration template.
Save	Click to save the changes to the configuration template.
Grouped by	Displayed if you have chosen to display the attributes as groups.
Total	Displays the total number of attributes in the template.
Modified	Displays the number of attributes you have modified.

Field	Description
Deploy	Select to deploy an attribute. If you do not select an attribute, the attribute value is not deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the value of an attribute.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Group	Displays the group the attribute belongs to.

Related link

[Viewing device deployment template attributes](#)

IOA VLAN Attributes

The fields displayed in the **IOA VLAN Attributes** pane of the **Deployment Portal** are described in the following table.

Table 70. IOA VLAN Attributes

Field	Description
Undo	Click to undo the changes made to the IOA template.
Save	Click to save the changes to the IOA template.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Deploy	Select to deploy an attribute. If an attribute is not selected, the attribute value will not be deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the attributes.
NIC	Displays the Fully Qualified Device Descriptor (FQDD) of the NIC.
Fabric	Displays the fabric associated with a specific slot of the chassis. The fabric is identified by a combination of the group name (A, B, or C) and slot number (1 or 2).

Field	Description
Tagged VLAN(s)	Field to enter the tagged VLANs values.
Untagged VLAN	Field to enter the untagged VLAN value.

Device Configuration Setup Wizard

The **Device Configuration Setup Wizard** guides you through the steps to get started with the configuration deployment and compliance tasks.

 **NOTE:** The Device Configuration Setup Wizard is only displayed if you try to perform a task that is missing required information.

File Share Settings

The fields displayed in the **File Share Settings** page are described in the following table.

Table 71. File Share Setting

Field	Description
Domain \ Username	User name to access the file share on the server running OpenManage Essentials.
Password	Password to access the file share on the server running OpenManage Essentials.
File Share Status	Indicates the status of the deployment file share configuration.
Allow using file share for Device Configuration feature on server	Allows using file share for device configuration features on the server.

Add devices to repurpose and bare-metal devices group

 **NOTE:** Adding devices to the repurpose and bare-metal devices group is applicable only for the device configuration deployment task.

 **NOTE:** Servers that you add to the repurpose and bare-metal devices group must have the Server Configuration Management license installed.

The **Add Devices to Repurpose and Bare Metal Device Group** page displays the servers and chassis that you can add to the repurpose and bare-metal devices group.

Add Network

Table 72. Add Network

Network types	Description
Name	Name for the network.
Description	Description for the network.
VLAN ID	VLAN IDs for the network. The valid VLAN IDs are: 1 to 4000 and 4021 to 4094.
Network Type	Type of the network.

Network Types

Table 73. Network Types

Network types	Description
Bronze General Purpose	Used for low priority data traffic.
Gold General Purpose	Used for high priority data traffic
Silver General Purpose	Used for standard or default priority data traffic
Platinum General Purpose	Used for extremely high priority data traffic
Cluster Interconnect	Used for cluster heartbeat VLANs
Hypervisor Management	Used for hypervisor management connections such as the ESXi management VLAN
iSCSI Storage	Used for iSCSI VLANs
FCoE Storage	Used for FCoE VLANs
Data Replication Storage	Used for VLANs supporting storage data replication such as for VMware Virtual Storage Area Network (VSAN)
VM Migration	Used for VLANs supporting vMotion and similar technologies
VMWare FT Logging	Used for VLANs supporting VMware Fault Tolerance

Create Template Wizard

The following table describes the fields displayed in the **Create Template Wizard**.

Table 74. Create Template Wizard

Field	Description
Name	Provide the name of the configuration template.
Create from File	Select if you want to create the configuration template from an existing file.
Create from Device	Select if you want to create the configuration template from a reference server or chassis.
Device Type	Select a Server , Chassis , MX Chassis , or an IOA based on the device from which you want to create the configuration template.
All Applicable Devices	Displays the devices from which you can create a configuration template.
Execution Credentials	
User Name	Provide the user name required to execute the task on the device.
Password	Provide the password required to execute the task on the device.

Related links

[Creating a device deployment template from a device configuration file](#)

[Creating a device deployment template from a reference device](#)

Create Virtual Input-Output Pool Wizard

The **Create Virtual I/O Pool Wizard** guides you through the creation of a pool of one or more virtual I/O identity types. OpenManage Essentials utilizes the virtual I/O identities from the pool to assign a unique identity to the network interfaces of a server. The fields displayed on the various pages of the wizard are described in the following sections.

 **NOTE: Creating a virtual I/O pool is a prerequisite for automatically assigning and managing the virtual identities of the network interfaces of a server.**

Related links

[Name and Description](#)
[Ethernet Identities](#)
[FCoE Node Name Identities](#)
[FCoE Port Name Identities](#)
[iSCSI IQN Identities](#)
[Summary](#)

Name and Description

The **Name and Description** page allows you to provide a name and description for the task.

The fields displayed on the **Name and Description** page of the **Create Virtual I/O Pool Wizard** are described in the following table.

Table 75. Name and Description

Field	Description
Name	Provide a name for the virtual I/O pool.
Description (optional)	Provide a description for the virtual I/O pool.

Related link


[Create Virtual Input-Output Pool Wizard](#)


Ethernet Identities

The **Ethernet Identities** page allows you to generate or import Media Access Control (MAC) addresses to the virtual I/O pool. MAC addresses are required for Ethernet (LAN) communications.

The fields displayed on the **Ethernet Identities** page of the **Create Virtual I/O Pool Wizard** are described in the following table.

Table 76. Ethernet Identities

Field	Description
Include MAC addresses in this pool	Select to include MAC addresses in the virtual I/O pool.
Specify the start address	Select to specify the start address for the MAC addresses that will be generated.
Number of Identities	Set the number of identities that you want to predefine in the MAC addresses that will be generated.
Import from file	Select to import MAC addresses from a .csv file.
Import	Click to open the wizard used to import MAC addresses from a .csv file.  NOTE: The .csv must include only one address or identity per line.
View	Click to view the MAC addresses in the virtual I/O pool.

Field	Description
	 NOTE: You can only view MAC addresses that you have already imported from a .csv file.

Related link



[Create Virtual Input-Output Pool Wizard](#)

FCoE Node Name Identities

The **FCoE Node Name Identities** page allows you to generate or import World Wide Node Name (WWNN) identities to the virtual I/O pool. WWNN identities are required for Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) communications.

The fields displayed on the **FCoE Node Name Identities** page of the **Create Virtual I/O Pool Wizard** are described in the following table.

Table 77. FCoE Node Name Identities

Field	Description
Include Fibre Channel WWNN Identities in the pool	Select to include WWNN identities in the virtual I/O pool.
Specify the start address	Select to specify the start address for the WWNN identities that will be generated.
Number of Identities	Set the number of identities that you want to predefine in the WWNN identities that will be generated.
Import from file	Select to import WWNN identities from a .csv file.
Import	Click to open the wizard used to import WWNN identities from a .csv file.  NOTE: The .csv must include only one address or identity per line.
View	Click to view the WWNN identities in the virtual I/O pool.  NOTE: You can only view WWNN identities that you have already imported from a .csv file.

Related link

[Create Virtual Input-Output Pool Wizard](#)



FCoE Port Name Identities

The **FCoE Port Name Identities** page allows you to generate or import World Wide Port Name (WWPN) identities to the virtual I/O pool. WWPN identities are required for Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) communications.

The fields displayed on the **FCoE Port Name Identities** page of the **Create Virtual I/O Pool Wizard** are described in the following table.

Table 78. FCoE Port Name Identities

Field	Description
Include Fibre Channel WWPN Identities in the pool	Select to include WWPN identities in the virtual I/O pool.
Specify the start address	Select to specify the start address for the WWPN identities that will be generated.
Number of Identities	Set the number of identities that you want to predefine in the WWPN identities that will be generated.

Field	Description
Import from file	Select to import WWPN identities from a .csv file.
Import	Click to open the wizard used to import WWPN identities from a .csv file.  NOTE: The .csv must include only one address or identity per line.
View	Click to view the WWPN identities in the virtual I/O pool.  NOTE: You can only view WWPN identities that you have already imported from a .csv file.

Related link




[Create Virtual Input-Output Pool Wizard](#)

iSCSI IQN Identities

The **iSCSI IQN Identities** page allows you to generate or import iSCSI Qualified Name (IQN) identities to the virtual I/O pool. The IQN identities are required to support boot-from-SAN using the iSCSI protocol.

The fields displayed on the **iSCSI IQN Identities** page of the **Create Virtual I/O Pool Wizard** are described in the following table.

Table 79. iSCSI IQN Identities

Field	Description
Include IQN Identities in the Pool	Select to include IQN identities in the virtual I/O pool.
Specify a prefix to allocate from	Select to specify a prefix for the IQN identities that will be generated.  NOTE: The typical iSCSI IQN format is: <i>iqn.date.domainname-in-reverse:storage-identifier</i>. For example, <i>iqn.2001-04.com.example:storage.disk2.sys1.xyz</i>.
Import from file	Select to import IQN identities from a .csv file.
Import	Click to open the wizard used to import IQN identities from a .csv file.  NOTE: The .csv must include only one address or identity per line.
View	Click to view the IQN identities in the virtual I/O pool.  NOTE: You can only view IQN identities that you have already imported from a .csv file.

Related link


[Create Virtual Input-Output Pool Wizard](#)

Summary

The **Summary** page displays the definitions you provided for the create virtual I/O pool task.

The fields displayed on the **Summary** page are described in the following table.

Table 80. Summary

Field	Description
Name	Displays the task name.
Ethernet Definition	Displays the MAC address definition.
Number of Ethernet Identities	Displays the virtual I/O pool size of the ethernet identities.
FCoE WWNN Definition	Displays the WWNN identity definition.
Number of FCOE WWNN Identities	Displays the virtual I/O pool size of the WWNN identities.
FCoE WWPN Definition	Displays the WWPN identity definition.
Number of FCOE WWPN Identities	Displays the virtual I/O pool size of the WWPN identities.
IQN Definition	Displays the IQN definition of the iSCSI initiator.
Number of iSCSI IQN Identities	Displays the virtual I/O pool size of the iSCSI IQN identities.  NOTE: The Number of iSCSI IQN Identities is displayed only when the iSCSI IQN identities are imported from a .csv file.

Related link

[Create Virtual Input-Output Pool Wizard](#)

Virtual Input-Output Pools

The **Virtual I/O Pools** page displays details about all the virtual I/O pools you have created.

The fields displayed on the **Virtual I/O Pools** page are described in the following table.

Table 81. Virtual I/O Pools

Field	Description
Grouped by	Displays the grouping you have selected for displaying the details of the virtual I/O pools.
Locked	Displays if the virtual I/O pool is locked.
Name	Displays the name of the virtual I/O pool.
Number of Identities	Displays the total number of identities of the virtual I/O pool.
Total Identities in use	Displays the total number of virtual I/O identities that are either assigned or deployed to target devices.

Virtual Input-Output Pool Summary

The **Virtual I/O Pool Summary** page displays details about the virtual I/O pool that you have selected.

The fields displayed on the **Virtual I/O Pool Summary** page are described in the following table.

Summary

Table 82. Summary

Field	Description
Grouped by	Displays the grouping you have selected for displaying the details of the virtual I/O pool.
Identity Type	Displays the virtual identity type included in the virtual I/O pool.
Range Information	Displays the definition that you provided for the virtual identity type.
Number of Identities	Displays the total number of identities of the virtual I/O pool.
Total Identities in use	Displays the total number of virtual I/O identities that are either assigned or deployed to target devices.

Devices with Identities

Table 83. Devices with Identities

Field	Description
Grouped by	Displays the grouping that you selected for displaying the details of the devices.
Device Name	Displays the name of the device.
Service Tag or Node ID	Displays the unique identifier assigned to the device.
Total Assigned Identities	Displays the total number of virtual I/O identities assigned to the device.
Total Deployed Identities	Displays the total number of virtual I/O identities deployed on the device.
Total Identities in use	Displays the total number of virtual I/O identities that are either assigned or deployed on the device.
Is Device Deleted	Displays if the device was deleted from OpenManage Essentials after it was deployed with virtual I/O identities.
Template Name	Displays the name of the template assigned to the device.
Compute Pool	Displays the name of the compute pool to which the device belongs.
Last Deploy Time	Displays the time stamp of the last deployment on the device.
Model	Displays the model name of the device, if available. For example, PowerEdge R710.

Create Compute Pool Wizard

The **Create Compute Pool Wizard** guides you through the creation of a pool of servers that you want to use for a specific purpose. The fields displayed on the various pages of the wizard are described in the following sections.

Related links

[Name and Description](#)

[Select Template](#)

[Select ISO Location](#)

[Select Virtual Input-Output Pool](#)

[Select Devices](#)

[Edit Attributes](#)

[Summary](#)

Name and Description

The **Name and Description** page allows you to provide a name and description for the task.

The fields displayed on the **Name and Description** page of the **Create Compute Pool Wizard** are described in the following table.

Table 84. Name and Description

Field	Description
Name	Provide a name for the compute pool.
Description (optional)	Provide a description for the compute pool.

Related link

[Create Compute Pool Wizard](#)


Select Template

The **Select Template** page allows you to select the template that you want to assign to the compute pool.

 **NOTE:** Selecting a template is optional. You can select a template at a later time, either by editing the compute pool or while deploying a server.

The fields displayed on the **Select Template** page of the **Create Compute Pool Wizard** are described in the following table.

Table 85. Select Template


Field	Description
Select Template for the Compute Pool	Select to assign a template to the compute pool.
Server Templates	Displays a list of templates that you can assign to the compute pool. Click the template name to select a template.  NOTE: Only templates that are not assigned to any compute pool are displayed.

Related link

[Create Compute Pool Wizard](#)

Select ISO Location

The **Select ISO Location** page allows you to provide the details of a bootable operating system ISO file.

 **NOTE:** Providing the ISO file details is applicable only for target servers that do not have virtual I/O identities. Typically, servers with virtual I/O identities are expected to boot from a SAN.

The fields displayed on the **Select ISO Location** page of the **Create Compute Pool Wizard** are described in the following table.

Table 86. Select ISO Location

Field	Description
Boot Compute Pool from Network ISO	Select to boot devices included in the compute pool from an operating system ISO file.
ISO Filename	Provide the name of the ISO file.
Share IP	Provide the IP address of the network share where the ISO file is available.
Share Name	Provide the name of the network share where the ISO file is available.

Related link


[Create Compute Pool Wizard](#)

Select Virtual Input-Output Pool

The **Select Virtual I/O Pool** page allows you to select the method of assigning the virtual I/O identity on the target servers.

The fields displayed on the **Select Virtual I/O Pool** page are described in the following table.

Table 87. Select Virtual I/O Pool

Field	Description
User-defined I/O assignment	Select to manually assign the virtual I/O identities.
Automatic I/O assignment	Select to allow OpenManage Essentials to automatically assign virtual I/O identities to the target servers. The virtual I/O identities are assigned from the virtual I/O pool that you select.  NOTE: The virtual I/O pools are available for selection only if you have already created the virtual I/O pools.

Related link

[Create Compute Pool Wizard](#)

Select Devices

The **Select Devices** page allows you to select the servers you want to include in the compute pool.

 **NOTE: Only servers that you have added to the Repurpose and Bare Metal group are available for selection.**

The **Select Devices** page displays a tree-view of the servers that you can include in the compute pool. You can select one or more servers for inclusion in the compute pool.


Related link

[Create Compute Pool Wizard](#)

Edit Attributes

The **Edit Attributes** page enables you to edit the attributes of the selected device configuration template, device-specific attributes, and the IOA VLAN attributes.

 **NOTE: The Edit Attributes page is only displayed if you have selected or assigned a template for compute pool.**

 **NOTE: Editing the attributes of the template is optional. You can edit the attributes of the template at a later time, either by editing the compute pool or while deploying the server.**

Template Attributes

The fields displayed on the **Template Attributes** tab are described in the following table.

Table 88. Template Attributes

Field	Description
Grouped by	Displayed if you choose to display the attributes as groups.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Attributes for	Displays the name of the selected device configuration template.
Device Specific Attributes for	Displays the following: <ul style="list-style-type: none">For a deployment task — The device name, Service Tag, and device model.For an auto deployment task — The Service Tag of the device to be discovered later.
Deploy	Select to deploy an attribute. If you do not select an attribute, the attribute value is not deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the value of the attribute.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Undo	Click to undo the changes made to the configuration template.
Save	Click to save the changes to the configuration template.

IOA VLAN Attributes

The fields displayed on the **IOA VLAN Attributes** tab are described in the following table.

Table 89. IOA VLAN Attributes

Field	Description
IOA VLAN Attributes for Template	Displays the name of the selected template.
Total	Displays the total number of attributes.

Field	Description
Modified	Displays the number of attributes that you have modified.
Deploy	Select to deploy an attribute. If an attribute is not selected, the attribute value will not be deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the attributes.
NIC	Displays the Fully Qualified Device Descriptor (FQDD) of the NIC.
Fabric	Displays the fabric associated with a specific slot of the chassis. The fabric is identified by a combination of the group name (A, B, or C) and slot number (1 or 2).
Tagged VLAN(s)	Displays the list of tagged VLANs for the selected fabric.
Untagged VLAN	Displays the untagged VLAN for the selected fabric.
Undo	Click to undo the changes made to the IOA VLAN attributes of the selected template.
Save	Click to save the changes to the IOA VLAN attributes of the selected template.

Device Specific Attributes

The fields displayed on the **Device Specific Attributes** tab are described in the following table.

Table 90. Template Attributes

Field	Description
Grouped by	Displayed if you choose to display the attributes as groups.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Attributes for	Displays the name of the selected device configuration template.
Device Specific Attributes for	Displays the following: <ul style="list-style-type: none"> For a deployment task — The device name, Service Tag, and device model. For an auto deployment task — The Service Tag of the device to be discovered later.
Deploy	Select to deploy an attribute. If you do not select an attribute, the attribute value is not deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the value of the attribute.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.

Field	Description
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Undo	Click to undo the changes made to the configuration template.
Save	Click to save the changes to the configuration template.

Import/Export Device Specific Attributes

The fields displayed on the **Import/Export Device Specific Attributes** window are described in the following table.

Table 91. Import/Export Device Specific Attributes

Field	Description
Export Selected Device	Click to export the device specific attributes for the selected device to a .csv file.
Export All Devices	Click to export the device specific attributes for all selected devices to a .csv file.
Import	Click to import the device-specific attributes.
File Requirements and Info	Displays the requirements of the .csv file you must use to import device-specific attributes.
View Logs	Displays the user interface logs.
Close	Click to close the Import/Export Device Specific Attributes window.

Identity Attributes

The fields displayed on the **Identity Attributes** tab are described in the following table.

Table 92. Identity Attributes

Field	Description
Attributes for Template	Displays the selected device configuration template.
Grouped by	Displayed if you choose to display the attributes as groups. By default, the attributes are grouped by Section .
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Deploy	Select to deploy an attribute. If an attribute is not selected, the attribute value will not be deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box on the Deploy column header.

Field	Description
Modified	Displays if you have modified the value of the attribute.
Identity Impact	Displays if the identity attribute will be automatically generated.
Status	Displays the status of the generation of the identity attribute. An Error status is displayed if the selected virtual I/O pool either does not contain the virtual I/O attribute or does not have sufficient attributes.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Group	Displays the logical group that the attribute belongs to.
Assign Identities	Click to automatically assign virtual I/O identities to the target devices.
Undo	Click to undo the changes made to the configuration template.
Save	Click to save the changes to the configuration template.
Import/Export	Displays the Import/Export Device Specific Attributes window.

Identity Assignments

The fields displayed on the **Identity Assignments** tab are described in the following table.

 **NOTE:** The Identity Assignments tab is displayed only when you click **Assign Identities** on the **Identity Attributes** tab.

Table 93. Identity Assignments

Field	Description
Device	Displays the selected device configuration template.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.

Related link

[Create Compute Pool Wizard](#)

Summary

The **Summary** page displays the details you have provided for creating the compute pool.

The fields displayed on the **Summary** page are described in the following table.

Table 94. Summary

Field	Description
Name	Displays the task name.
Selected Template	Displays the name of the template you have selected.
ISO Filename	Displays the name of the ISO file.
Share IP	Displays the IP address of the network share where the ISO file is available.
Share Name	Displays the name of the network share where the ISO file is available.
Identity Assignment	Displays the type of I/O identity assignment that you have selected.
Associated Devices	Displays the devices that you have selected for inclusion in the compute pool.
Device Specific Attributes	Displays if the device-specific attributes are set.
Configure VLANs on IOAs	Displays if you have selected to configure the VLANs on the IOAs.

Related link

[Create Compute Pool Wizard](#)

Compute Pool Summary

The fields displayed on the **Compute Pool Summary** page are described in the following table.

Table 95. Compute Pool Summary

Field	Description
Grouped by	Displays the grouping you have selected for displaying the details of the compute pools.
Locked	Displays if the compute pool is locked.
Pool Name	Displays the name of the compute pool.
Server Template	Displays the name of the template that is assigned to the compute pool.
Virtual I/O Pool	Displays the name of the virtual I/O pool that is assigned to the compute pool.
Total servers	Displays the total number of servers in the compute pool.
Deployed servers	Displays the number of servers in the compute pool that have been deployed.

Compute Pool Details

The fields displayed on the **Compute Pool Details** page are described in the following table.

Table 96. Compute Pool Details

Field	Description
Template	Displays the name of the template assigned to the compute pool. Click the template name to view the attributes of the template.
Virtual I/O Pool	Displays the name of the virtual I/O pool that is assigned to the compute pool.
Network ISO Image	Displays the name of the network ISO file assigned to the compute pool.
Device count	Displays the total number of servers in the compute pool.
Deployed count	Displays the number of servers in the compute pool that have been deployed.
Grouped by	Displays the grouping you have selected for displaying the compute pool details.
Device	Displays the name of the server.
Deployed	Displays if the server is deployed.
Last Deploy Time	Displays the time stamp of the last deployment on the server.

Server Details

The fields displayed on the server **Details** page are described in the following table.

Table 97. Server Details

Field	Description
Server Template	Displays the name of the template that is assigned to the server.
Virtual I/O Pool	Displays the name of the virtual I/O pool that is assigned to the server.
Inventory	Displays an inventory of the configuration attributes of the server.
Profile	Displays the template attributes, device-specific attributes, and virtual I/O identity attributes that were last deployed on the server.

Deploy Template Wizard

The **Deploy Template Wizard** guides you through the steps to deploy a configuration template and/or boot to a network ISO image. The steps displayed in the wizard may vary based on the deploy option you select. The fields displayed in the various pages of the wizard are described in the following sections.

Related links


[Name and Deploy Options](#)
[Select Template](#)
[Select Devices](#)
[Select ISO Location](#)
[Edit Attributes](#)
[Options](#)
[Set Schedule](#)
[Preview](#)
[Summary](#)

Name and Deploy Options

The **Name and Deploy Options** page enables you to provide a name for the task and also select the deployment options.

The fields displayed in the **Name and Deploy Options** page of the **Deploy Template Wizard** are described in the following table.

Table 98. Name and Deploy Options

Field	Description
Task Name	Provide a name for the task.
Deploy Target	
Compute Pool	Select to deploy a device configuration template on one or more devices in a compute pool.
Select a Compute Pool	Select a compute pool on which you want to deploy a device configuration template.
Bare metal	Select to deploy the device configuration template on one or more devices in the Repurpose and Bare Metal group.
Select Deploy Options	
Deploy Template	Select to deploy a device configuration template to one or more devices.
Boot to Network ISO	Select to boot each target device from a specified network ISO image.  NOTE: If the Deploy Template option is also selected, the boot-to-ISO operation starts after the deployment is completed.

Related link

[Deploy Template Wizard](#)





Select Template

The **Select Template** page enables you to select the template you want to deploy on the target devices.

 **NOTE: The Select Template page is only displayed if you select the Deploy Template option in the Name and Deploy Options or Select Deploy Options page.**

The fields displayed in the **Select Template** page are described in the following table.

Table 99. Select Template

Field	Description
Server Templates	Displays the server configuration templates that you have either created or cloned.
Chassis Templates  NOTE: If you select both Deploy Template and Boot to Network ISO in the Name and Deploy Options or Select Deploy Options page, the Chassis Templates option is disabled.	Displays the chassis configuration templates that you have either created or cloned.
IOA Templates  NOTE: If you select Compute Pool in the Name and Deploy Options page, the IOA Templates option is not displayed.  NOTE: If you select both Deploy Template and Boot to Network ISO in the Name and Deploy Options page, the IOA Templates option is disabled.	Displays the IOA configuration templates that you have either created or cloned.
MX Chassis Templates  NOTE: If you select both Deploy Template and Boot to Network ISO in the Name and Deploy Options or Select Deploy Options page, the MX Chassis Templates option is disabled.	Displays the MX chassis configuration templates that you have either created or cloned.

Related link

[Deploy Template Wizard](#)

Select Devices

The **Select Devices** page enables you to select target devices for deployment.

The **Select Devices** page displays the **Repurpose and Bare Metal Devices** tree-view that includes the target devices. You can select more than one target device for deployment.

Related link

[Deploy Template Wizard](#)

Select ISO Location

The **Select ISO Location** page enables you to provide the details of the ISO file.

 **NOTE:** The **Select ISO Location** page is only displayed if you select the **Boot to Network ISO** option on the **Name and Deploy Options** or **Select Deploy Options** page.

The fields displayed in the **Select ISO Location** page are described in the following table.

Table 100. Select ISO Location

Field	Description
ISO Filename	
ISO Filename	Provide the name of the ISO file.
Share Location	

Field	Description
Share IP	Provide the IP address of the network share where the ISO file is available.
Share Name	Provide the name of the network share where the ISO file is available.
Share Credentials	
Share Username	Provide the user name required to access the network share.
Share Password	Provide the password required to access the network share.

Related link


[Deploy Template Wizard](#)

Select Virtual Input-Output Pool

The **Select Virtual I/O Pool** page allows you to select the method of assigning the virtual I/O identity on the target servers.

The fields displayed on the **Select Virtual I/O Pool** page are described in the following table.

Table 101. Select Virtual I/O Pool


Field	Description
User-defined I/O assignment	Select to manually assign the virtual I/O identities.
Automatic I/O assignment	Select to allow OpenManage Essentials to automatically assign virtual I/O identities to the target servers. The virtual I/O identities are assigned from the virtual I/O pool that you select.  NOTE: The virtual I/O pools are available for selection only if you have already created the virtual I/O pools.

Related link

[Create Compute Pool Wizard](#)

Edit Attributes

The **Edit Attributes** page enables you to edit the attributes of the selected configuration template, device-specific attributes, and the IOA VLAN attributes.

 **NOTE: The Edit Attributes page is only displayed if you select the Deploy Template option in the Name and Deploy Options or Deploy Options page.**

Template Attributes

 **NOTE: The Template Attributes tab will not be displayed if you select the IOA Template option for deployment.**

The fields displayed in the **Template Attributes** tab of the **Edit Attributes** page are described in the following table.

Table 102. Template Attributes

Field	Description
Grouped by	Displayed if you choose to display the attributes as groups.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Attributes for	Displays the name of the selected device configuration template.

Field	Description
Device Specific Attributes for	Displays the following: <ul style="list-style-type: none"> For a deployment task — The device name, Service Tag, and device model. For an auto deployment task — The Service Tag of the device to be discovered later.
Deploy	Select to deploy an attribute. If you do not select an attribute, the attribute value is not deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the value of the attribute.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Undo	Click to undo the changes made to the configuration template.
Save	Click to save the changes to the configuration template.

IOA VLAN Attributes

The fields displayed on the **IOA VLAN Attributes** tab are described in the following table.

Table 103. IOA VLAN Attributes

Field	Description
IOA VLAN Attributes for Template	Displays the name of the selected template.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Deploy	Select to deploy an attribute. If an attribute is not selected, the attribute value will not be deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the attributes.
NIC	Displays the Fully Qualified Device Descriptor (FQDD) of the NIC.

Field	Description
Fabric	Displays the fabric associated with a specific slot of the chassis. The fabric is identified by a combination of the group name (A, B, or C) and slot number (1 or 2).
Tagged VLAN(s)	Displays the list of tagged VLANs for the selected fabric.
Untagged VLAN	Displays the untagged VLAN for the selected fabric.
Undo	Click to undo the changes made to the IOA VLAN attributes of the selected template.
Save	Click to save the changes to the IOA VLAN attributes of the selected template.

Device Specific Attributes

The fields displayed on the **Device Specific Attributes** tab are described in the following table.

Table 104. Device Specific Attributes

Field	Description
Select Devices	Displays the devices that you have selected for deployment. You can select a device to view the attributes specific to that device.
Device Specific Attributes for	Displays the model number and Service Tag of the selected device.
Grouped by	Displayed if you have chosen to display the attributes as groups.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Deploy	Select to deploy an attribute. If an attribute is not selected, the attribute value will not be deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the value of the attribute.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Undo	Click to undo the changes made to the configuration template.

Field	Description
Save	Click to save the changes to the configuration template.
Import/Export	Displays the Import/Export Device Specific Attributes window.

Import/Export Device Specific Attributes

The fields displayed on the **Import/Export Device Specific Attributes** window are described in the following table.

Table 105. Import/Export Device Specific Attributes

Field	Description
Export Selected Device	Click to export the device specific attributes for the selected device to a .csv file.
Export All Devices	Click to export the device specific attributes for all selected devices to a .csv file.
Import	Click to import the device-specific attributes.
File Requirements and Info	Displays the requirements of the .csv file you must use to import device-specific attributes.
View Logs	Displays the user interface logs.
Close	Click to close the Import/Export Device Specific Attributes window.

Identity Attributes

The fields displayed on the **Identity Attributes** tab are described in the following table.

Table 106. Identity Attributes

Field	Description
Attributes for Template	Displays the selected device configuration template.
Grouped by	Displayed if you choose to display the attributes as groups. By default, the attributes are grouped by Section .
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Deploy	Select to deploy an attribute. If an attribute is not selected, the attribute value will not be deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box on the Deploy column header.
Modified	Displays if you have modified the value of the attribute.
Identity Impact	Displays if the identity attribute will be automatically generated.
Status	Displays the status of the generation of the identity attribute. An Error status is displayed if the selected virtual I/O pool either does not contain the virtual I/O attribute or does not have sufficient attributes.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.

Field	Description
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Group	Displays the logical group that the attribute belongs to.
Assign Identities	Click to automatically assign virtual I/O identities to the target devices.
Undo	Click to undo the changes made to the configuration template.
Save	Click to save the changes to the configuration template.
Import/Export	Displays the Import/Export Device Specific Attributes window.

Identity Assignments

The fields displayed on the **Identity Assignments** tab are described in the following table.



NOTE: The Identity Assignments tab is displayed only when you click Assign Identities on the Identity Attributes tab.

Table 107. Identity Assignments

Field	Description
Device	Displays the selected device configuration template.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.

Related links

[Deploy Template Wizard](#)

[Importing Device Specific Attributes](#)

[Exporting Device Specific Attributes](#)

Options



The **Options** page enables you to select the options you can use to verify if the IOA template is compatible with the target devices.



NOTE: The Options page is only displayed if you select an IOA template in the Select Template page.

The fields displayed in the **Options** page of the **Deploy Template Wizard** are described in the following table.

Table 108. Options

Field	Description
Perform pre-check only	<p>Select Perform pre-check only to only verify (not deploy) if the device configuration template will be deployed successfully.</p> <p> NOTE: If the Perform pre-check only option is selected, by default the Continue on warnings option is disabled.</p>
Continue on warnings	<p>Select Continue on warnings to continue deploying the template even if the template is incompatible with the target devices.</p> <p> NOTE: When this option is selected, warnings (if any) will be ignored and the deployment task runs even if the device configuration template is incompatible.</p>

Related link


[Deploy Template Wizard](#)

Set Schedule

The **Set Schedule** page enables you to set the date and time at which you want to deploy the task.

The fields displayed in the **Set Schedule** page are described in the following table.

Table 109. Set Schedule

Field	Description
Run Now	Select to run the deployment task immediately.
Run At	Select to schedule the deployment task.
Execution Credentials	
User Name	Provide the user name required to run the task.
Password	Provide the password required to run the task.
IOA Credentials	<p> NOTE: The IOA Credential fields are displayed only in the following scenarios:</p> <ul style="list-style-type: none"> The selected device configuration template was created from a blade server. You have selected to deploy VLAN attributes on the IOA.
User Name	Provide the IOA administrator user name required to deploy the VLAN attributes.
Password	Provide the IOA administrator password required to deploy the VLAN attributes.

Related link

[Deploy Template Wizard](#)

Preview

 **NOTE: The preview activity is optional.**

The **Preview** page allows you to view the attributes of the selected configuration template that will not be applied successfully on a target device. The preview activity sends the pending configuration to each target device, but for validation only (no configuration

changes are made). Each device verifies the validity of the settings in the configuration and identifies any problems. The verification can identify problems with attribute values themselves, or problems based on inter-attribute dependencies. For example, creating a device configuration template from a PowerEdge R720 server and deploying the template on a PowerEdge R620 server would result in errors. Running the preview allows you to identify the attributes that will not be deployed successfully. After identifying those attributes, if required, you can clear those attributes from the template and then deploy the template.

 **NOTE: The preview activity identifies many problems; however, some problems cannot be determined before the actual deployment.**

Click the **Preview** button to validate the attributes of the device configuration template with the selected device.

Related link

[Deploy Template Wizard](#)

Summary

The **Summary** page displays the options you have selected for the deployment task.

The fields displayed in the **Summary** page are described in the following table.

Table 110. Summary

Field	Description
Task Name	Displays the task name.
Deploy Template	Displays if the task will deploy a configuration template.
Boot to Network ISO	Displays if the task will boot to a network ISO image.
Deploy Target	Displays the target devices that you have selected.
Selected Template	Displays the configuration template selected for deployment.
Device Specific Attributes	Displays if the device-specific attributes are set.
ISO Filename	Displays the name of the ISO file.
Share IP	Displays the IP address of the network share where the ISO file is available.
Share Name	Displays the name of the network share where the ISO file is available.
Share Username	Displays the user name provided to access the network share.
Identity Assignment	Displays the type of I/O identity assignment that you have selected.
Virtual IO Pool	Displays the name of the virtual IO pool to which the device belongs.
Associated Devices	Displays the selected target devices.
Configure VLANs on IOA	Displays if you have selected to deploy VLAN attributes on the IOA.
Perform pre-check only	Displays if you have selected the Perform pre-check only option.
Continue on warnings	Displays if you have selected the Continue on warnings option.
Schedule	Displays the schedule selected for the task.

Related link

[Deploy Template Wizard](#)

Setup Auto Deployment Wizard

The **Setup Auto Deployment** wizard guides you through the steps to deploy a configuration template and/or boot to a network ISO image on target devices that you will discover later. The steps displayed in the wizard may vary based on the deployment option you select. The fields displayed in the various pages of the wizard are described in the following sections.

Related links

[Select Deploy Options](#)

[Select Template](#)

[Select ISO Location](#)

[Import Service Tags or Node IDs](#)

[Edit Attributes](#)

[Execution Credentials](#)

[Summary](#)

Select Deploy Options

The **Select Deploy Options** page enables you to select the deployment options.


The fields displayed in the **Select Deploy Options** page of the **Setup Auto Deployment** wizard are described in the following table.

Table 111. Select Deploy Options

Field	Description
Deploy Target	
Compute Pool	Select to auto deploy the servers within a compute pool.
Select a Compute Pool	Select a compute pool on which you want auto deploy a device configuration template with virtual I/O identities.
Bare Metal	Select to auto deploy a device configuration template on bare metal servers.
Select Deploy Options	
Deploy Template	Select to auto deploy a device configuration template on the target servers.
Boot to Network ISO	Select to boot the target servers to a network ISO image.

Select Template


The **Select Template** page enables you to select the template you want to deploy on the target devices.

 **NOTE:** The **Select Template** page is only displayed if you select the **Deploy Template** option in the **Name and Deploy Options** or **Select Deploy Options** page.

The fields displayed in the **Select Template** page are described in the following table.

Table 112. Select Template

Field	Description
Server Template	Displays the server configuration templates that you have either created or cloned.
Chassis Template	Displays the chassis configuration templates that you have either created or cloned.

Field	Description
 NOTE: If you select both Deploy Template and Boot to Network ISO in the Name and Deploy Options or Select Deploy Options page, the Chassis Template option is disabled.	

Select ISO Location

The **Select ISO Location** page enables you to provide the details of the ISO file.

 **NOTE:** The **Select ISO Location** page is only displayed if you select the **Boot to Network ISO** option on the **Name and Deploy Options** or **Select Deploy Options** page.

The fields displayed in the **Select ISO Location** page are described in the following table.

Table 113. Select ISO Location

Field	Description
ISO Filename	
ISO Filename	Provide the name of the ISO file.
Share Location	
Share IP	Provide the IP address of the network share where the ISO file is available.
Share Name	Provide the name of the network share where the ISO file is available.
Share Credentials	
Share Username	Provide the user name required to access the network share.
Share Password	Provide the password required to access the network share.

Related link


[Deploy Template Wizard](#)

Select Virtual Input-Output Pool

The **Select Virtual I/O Pool** page allows you to select the method of assigning the virtual I/O identity on the target servers.

The fields displayed on the **Select Virtual I/O Pool** page are described in the following table.

Table 114. Select Virtual I/O Pool


Field	Description
User-defined I/O assignment	Select to manually assign the virtual I/O identities.
Automatic I/O assignment	<p>Select to allow OpenManage Essentials to automatically assign virtual I/O identities to the target servers. The virtual I/O identities are assigned from the virtual I/O pool that you select.</p> <p> NOTE: The virtual I/O pools are available for selection only if you have already created the virtual I/O pools.</p>

Related link

[Create Compute Pool Wizard](#)

Import Service Tags or Node IDs

The **Import Service Tags/Node IDs** page of the **Setup Auto Deployment** wizard displays the **Import** button. Click **Import** to import a .csv file that includes Service Tags or node IDs of devices that you will discover later.

 **NOTE:** On devices which have multiple compute nodes (such as the PowerEdge FM120x4), all of the compute nodes have the same Service Tag. Therefore, the node ID must be used to identify the specific compute node to use. In the .csv file, you must include the node IDs of the specific compute nodes that you want to auto deploy.

 **NOTE:** The Service Tags or node IDs that you want to import:

- Must be listed in the .csv file in a column titled 'ServiceTag', 'Service Tag', or 'Node ID'.
- Must be valid Service Tags or node IDs.
- Must not be Service Tags or node IDs of devices that are already discovered.


The following is an example of the .csv file format that contains Service Tags and node IDs:

	A
1	Service Tag
2	ABCD123
3	1DSZF23
4	HY3912B
5	GFEDCBaA
6	GFEDCBAb
7	GFEDCBaC
8	GFEDCBAd

Figure 27. Sample CSV file

Edit Attributes

The **Edit Attributes** page enables you to edit the attributes of the selected configuration template, device-specific attributes, and the IOA VLAN attributes.

 **NOTE:** The **Edit Attributes** page is only displayed if you select the **Deploy Template** option in the **Name and Deploy Options** or **Deploy Options** page.

Template Attributes

 **NOTE:** The **Template Attributes** tab will not be displayed if you select the **IOA Template** option for deployment.

The fields displayed in the **Template Attributes** tab of the **Edit Attributes** page are described in the following table.

Table 115. Template Attributes

Field	Description
Grouped by	Displayed if you choose to display the attributes as groups.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Attributes for	Displays the name of the selected device configuration template.
Device Specific Attributes for	Displays the following: <ul style="list-style-type: none">• For a deployment task — The device name, Service Tag, and device model.

Field	Description
	<ul style="list-style-type: none"> For an auto deployment task — The Service Tag of the device to be discovered later.
Deploy	Select to deploy an attribute. If you do not select an attribute, the attribute value is not deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the value of the attribute.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Undo	Click to undo the changes made to the configuration template.
Save	Click to save the changes to the configuration template.

IOA VLAN Attributes

The fields displayed on the **IOA VLAN Attributes** tab are described in the following table.

Table 116. IOA VLAN Attributes

Field	Description
IOA VLAN Attributes for Template	Displays the name of the selected template.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Deploy	Select to deploy an attribute. If an attribute is not selected, the attribute value will not be deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the attributes.
NIC	Displays the Fully Qualified Device Descriptor (FQDD) of the NIC.
Fabric	Displays the fabric associated with a specific slot of the chassis. The fabric is identified by a combination of the group name (A, B, or C) and slot number (1 or 2).

Field	Description
Tagged VLAN(s)	Displays the list of tagged VLANs for the selected fabric.
Untagged VLAN	Displays the untagged VLAN for the selected fabric.
Undo	Click to undo the changes made to the IOA VLAN attributes of the selected template.
Save	Click to save the changes to the IOA VLAN attributes of the selected template.

Device Specific Attributes

The fields displayed on the **Device Specific Attributes** tab are described in the following table.

Table 117. Device Specific Attributes

Field	Description
Select Devices	Displays the devices that you have selected for deployment. You can select a device to view the attributes specific to that device.
Device Specific Attributes for	Displays the model number and Service Tag of the selected device.
Grouped by	Displayed if you have chosen to display the attributes as groups.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Deploy	Select to deploy an attribute. If an attribute is not selected, the attribute value will not be deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the value of the attribute.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Undo	Click to undo the changes made to the configuration template.
Save	Click to save the changes to the configuration template.
Import/Export	Displays the Import/Export Device Specific Attributes window.

Import/Export Device Specific Attributes

The fields displayed on the **Import/Export Device Specific Attributes** window are described in the following table.

Table 118. Import/Export Device Specific Attributes

Field	Description
Export Selected Device	Click to export the device specific attributes for the selected device to a .csv file.
Export All Devices	Click to export the device specific attributes for all selected devices to a .csv file.
Import	Click to import the device-specific attributes.
File Requirements and Info	Displays the requirements of the .csv file you must use to import device-specific attributes.
View Logs	Displays the user interface logs.
Close	Click to close the Import/Export Device Specific Attributes window.

Identity Attributes

The fields displayed on the **Identity Attributes** tab are described in the following table.

Table 119. Identity Attributes

Field	Description
Attributes for Template	Displays the selected device configuration template.
Grouped by	Displayed if you choose to display the attributes as groups. By default, the attributes are grouped by Section .
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Deploy	Select to deploy an attribute. If an attribute is not selected, the attribute value will not be deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box on the Deploy column header.
Modified	Displays if you have modified the value of the attribute.
Identity Impact	Displays if the identity attribute will be automatically generated.
Status	Displays the status of the generation of the identity attribute. An Error status is displayed if the selected virtual I/O pool either does not contain the virtual I/O attribute or does not have sufficient attributes.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.

Field	Description
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Group	Displays the logical group that the attribute belongs to.
Assign Identities	Click to automatically assign virtual I/O identities to the target devices.
Undo	Click to undo the changes made to the configuration template.
Save	Click to save the changes to the configuration template.
Import/Export	Displays the Import/Export Device Specific Attributes window.

Identity Assignments

The fields displayed on the **Identity Assignments** tab are described in the following table.

 **NOTE:** The Identity Assignments tab is displayed only when you click **Assign Identities** on the **Identity Attributes** tab.

Table 120. Identity Assignments

Field	Description
Device	Displays the selected device configuration template.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.

Related links

[Deploy Template Wizard](#)

[Importing Device Specific Attributes](#)

[Exporting Device Specific Attributes](#)

Execution Credentials

The **Execution Credentials** page enables you to add and/or assign credentials that are required for running the auto deployment task on the target device. The fields displayed in the **Execution Credentials** page of the **Setup Auto Deployment** wizard are described in the following sections.

Credentials

The **Credentials** section displays a table that includes credentials that you have configured for target devices that you will discover later. The following are the fields displayed in the credentials table.

Table 121. Credentials

Field	Description
Add New Credentials	Click to open the Add Credentials window that enables you to provide credentials for target devices.
Description	Displays the description provided for the credentials.
Username	Displays the user name.
Password	Displays the password in a masked format.
Is Default	Displays a check box that you can select to associate the credentials to all new target devices.
Update	Displays an icon that you can click to edit the credentials.
Delete	Displays an icon that you can click to delete the credentials.

Devices

The **Devices** section displays a table that includes the target devices that you selected through the **Import Service Tags** page. The following are the fields displayed in the devices table.

Table 122. Devices

Field	Description
Device Name	Displays the Service Tag of the device.
Device Model	Displays the model name of the system, if available.
Execution Credentials	Displays the credentials that have been assigned to the device for running the deployment task.

IOA Credentials



NOTE: The IOA Credentials fields are displayed only in the following scenarios:

- The selected device configuration template was created from a modular server.
- You have selected to deploy VLAN attributes on the IOA.

Table 123. IOA Credentials

Field	Description
User Name	Provide the IOA administrator user name required to deploy the VLAN attributes.
Password	Provide the IOA administrator password required to deploy the VLAN attributes.

Related link

[Add Credentials](#)

Add Credentials

The **Add Credentials** window enables you to provide credentials required for running the auto deployment task on target devices.

The fields displayed in the **Add Credentials** window are described in the following table.

Table 124. Add Credentials

Field	Description
Description	Provide a description for the credentials.
Username	Provide the user name required to run the task on the target device.
Password	Provide the password required to run the task on the target device.
Default	Select to associate the credentials to all new target devices.

Summary

The **Summary** page displays the options you have selected for the auto deployment task.

The fields displayed in the **Summary** page are described in the following table.

Table 125. Summary

Field	Description
Name	Displays the task name.
Deploy Template	Displays if the task will deploy a configuration template.
Boot to Network ISO	Displays if the task will boot to a network ISO image.
Selected Template	Displays the configuration template selected for deployment.
ISO Filename	Displays the name of the ISO file.
Share IP	Displays the IP address of the network share where the ISO file is available.
Share Name	Displays the name of the network share where the ISO file is available.
Share Username	Displays the user name provided to access the network share.
Associated Service Tags/Node IDs	Displays the Service Tags or node IDs of the target devices.
Device Specific Attributes	Displays if the device-specific attributes are set.
Configure VLANs on IOA	Displays if you have selected to deploy VLAN attributes on the IOA.

Manage Auto Deployment Credentials

The **Manage Auto Deployment Credentials** page enables you to add and/or assign credentials that are required for running the auto deployment task on the target device. The fields displayed in the **Manage Auto Deployment Credentials** page are described in the following sections.

Credentials

The **Credentials** section displays a table that includes credentials that you have configured for the auto deployment task. The following are the fields displayed in the credentials table.

Table 126. Credentials

Field	Description
Add New Credentials	Click to open the Add Credentials window that enables you to provide credentials for target devices.
Description	Displays the description provided for the credentials.
Username	Displays the user name.
Password	Displays the password in a masked format.
Is Default	Displays a check box that you can select to associate the credentials to all new target devices.
Update	Displays an icon that you can click to edit the credentials.
Delete	Displays an icon that you can click to delete the credentials.

Devices

The **Devices** section displays a table that includes the target devices that you selected through the **Import Service Tags** page of the **Setup Auto Deployment** wizard. The following are the fields displayed in the devices table.

Table 127. Devices

Field	Description
Device Name	Displays the Service Tag of the device.
Device Model	Displays the model name of the system, if available.
Execution Credentials	Displays the credentials that have been assigned to the device for running the deployment task. You can use this field to assign the credentials required for running the auto deployment task on the device.

Related link

[Managing Auto Deployment Credentials](#)

Replace Server Wizard

The **Replace Server Wizard** guides you through the replacement of a production server with another server from within the same compute pool. The fields displayed on the various pages of the wizard are described in the following sections.

Related links

[Replacing a Server](#)
[Name](#)
[Source and Target](#)
[Review Source Attributes](#)
[Options](#)
[Credentials](#)
[Summary](#)

Name

The **Name** page allows you to provide a name for the task.

Related link


[Replace Server Wizard](#)

Source and Target

The **Source and Target** page allows you to select the source server and the target server for the replacement.

The fields displayed on the **Source and Target** page of the **Replace Server Wizard** are described in the following table.

Table 128. Source and Target

Field	Description
Select Source	Displays a tree-view of the servers within the compute pool that are already deployed.
Select Target	Displays all other servers within the same compute pool.  NOTE: Target servers are displayed only after you select the source server.

Related link

[Replace Server Wizard](#)

Review Source Attributes

The **Review Source Attributes** page allows you to view and edit the device configuration template, including the I/O identity attributes.

Template Attributes

The fields displayed on the **Template Attributes** tab are described in the following table.

Table 129. Template Attributes

Field	Description
Grouped by	Displayed if you choose to display the attributes as groups.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Undo	Click to undo the changes made to the device configuration template.
Save	Click to save the changes to the device configuration template.

IOA VLAN Attributes

The fields displayed on the **IOA VLAN Attributes** tab are described in the following table.

Table 130. IOA VLAN Attributes

Field	Description
IOA VLAN Attributes for Template	Displays the name of the selected template.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Deploy	Select to deploy an attribute. If an attribute is not selected, the attribute value will not be deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.
Modified	Displays if you have modified the attributes.
NIC	Displays the Fully Qualified Device Descriptor (FQDD) of the NIC.
Fabric	Displays the fabric associated with a specific slot of the chassis. The fabric is identified by a combination of the group name (A, B, or C) and slot number (1 or 2).
Tagged VLAN(s)	Displays the list of tagged VLANs for the selected fabric.
Untagged VLAN	Displays the untagged VLAN for the selected fabric.
Undo	Click to undo the changes made to the IOA VLAN attributes of the selected template.
Save	Click to save the changes to the IOA VLAN attributes of the selected template.

Device Specific Attributes

The fields displayed on the **Device Specific Attributes** tab are described in the following table.

Table 131. Template Attributes

Field	Description
Grouped by	Displayed if you choose to display the attributes as groups.
Total	Displays the total number of attributes.
Modified	Displays the number of attributes that you have modified.
Attributes for	Displays the name of the selected device configuration template.
Device Specific Attributes for	Displays the following: <ul style="list-style-type: none"> For a deployment task — The device name, Service Tag, and device model. For an auto deployment task — The Service Tag of the device to be discovered later.
Deploy	Select to deploy an attribute. If you do not select an attribute, the attribute value is not deployed on the target device and the current value will be retained on the target device. You can select all the attributes in the template by selecting the check box in the Deploy column header.

Field	Description
Modified	Displays if you have modified the value of the attribute.
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Undo	Click to undo the changes made to the configuration template.
Save	Click to save the changes to the configuration template.

Identity Assignments

The fields displayed on the **Identity Assignments** tab are described in the following table.

Table 132. Identity Assignments

Field	Description
Grouped by	Displayed if you choose to display the attributes as groups.
Section	Displays the component that the attribute belongs to. For example, NIC.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.

Related link

[Replace Server Wizard](#)



Options

The **Options** page allows you to select your preferences for the server replacement task.

The fields displayed on the **Options** page of the **Replace Server Wizard** are described in the following table.

Table 133. Options

Field	Description
Remove source from compute pool	Select to move the source server from the compute pool to the Repurpose and Bare Metal Devices group after the server is replaced.

Field	Description
	 NOTE: If this option is not selected, the source server is retained within the compute pool after the server is replaced.
Deploy to target even if virtual identities cannot be reclaimed from the source	<p>Select to reclaim the virtual I/O identities of the source server, even if the server is unreachable.</p>  NOTE: If the source server is not reachable and this option is: <ul style="list-style-type: none"> Not selected — The replace server task is unsuccessful. Selected — You may notice servers with duplicate I/O identities on the network, if the source server is added back to the network.

Related link

[Replace Server Wizard](#)

Credentials

The **Credentials** page allows you to provide the credentials of the source server and target server.

The fields displayed on the **Credentials** page of the **Replace Server Wizard** are described in the following table.

Table 134. Credentials

Section	Field	Description
Source Credentials	User Name	Provide the user name of the iDRAC of the source server.
	Password	Provide the password of the iDRAC of the source server.
Target Credentials	User Name	Provide the user name of the iDRAC of the target server.
	Password	Provide the password of the iDRAC of the target server.

Related link

[Replace Server Wizard](#)

Summary

The **Summary** page displays the options you have selected for the server replacement task.

The fields displayed on the **Summary** page of the **Replace Server Wizard** are described in the following table.

Table 135. Summary

Field	Description
Name	Displays the name that you have provided for the task.
Compute Pool	Displays the name of the compute pool that you have selected.
Source	Displays the name of the source server that you have selected.
Target	Displays the name of the target server that you have selected.

Field	Description
Configure VLANs on IOAs	Displays if you have selected to configure the VLANs on the IOAs.
Remove from Pool	Displays if you have chosen to remove the source server from the compute pool.
Force reclaim identities	Displays if you have chosen to reclaim the virtual I/O identities of the source server, even if source server is unreachable.
Schedule	Displays the predefined task schedule.

Related link

[Replace Server Wizard](#)

Reclaim Identities Wizard

The **Reclaim Identities Wizard** allows you to reclaim all managed virtual I/O identities from a server. The fields displayed on the various pages of the wizard are described in the following sections.

Related links

[Name](#)

[Select Devices](#)

[Identity Assignments](#)

[Options](#)

[Credentials](#)

[Summary](#)

[Reclaiming Deployed Virtual Input-Output Identities of a Server](#)

Name

The **Name** page allows you to provide a name for the task.

Related link

[Reclaim Identities Wizard](#)

Select Devices

The **Select Devices** page allows you to select devices from which you can reclaim the managed virtual I/O identities.

The fields displayed on the **Select Devices** page of the **Reclaim Identities Wizard** are described in the following tables.

Table 136. Select Devices

Field	Description
Device Name	Displays the name of the device.
Service Tag or Node ID	Displays the unique identifier assigned to the device.
Total of Identities in use	Displays the total number of identities that are deployed on the device.
Is Device Deleted	Displays if the device was deleted from OpenManage Essentials after it was deployed with virtual I/O identities.
Template Name	Displays the name of the device configuration template assigned to the device.
Compute Pool	Displays the name of the compute pool that the device belongs to.
Last Deploy Time	Displays the time stamp of the last deployment of the device.

Field	Description
Model	Displays the model name of the device, if available. For example, PowerEdge R710.

Related link

[Reclaim Identities Wizard](#)

Identity Assignments

The **Identity Assignments** page allows you to view the virtual I/O identities that are assigned to the selected server.

The fields displayed on the **Identity Assignments** page of the **Reclaim Identities Wizard** are described in the following tables.

Table 137. Identity Assignments

Field	Description
Device	Displays the name of the device.
Is Device Deleted	Displays if the device was deleted from OpenManage Essentials after it was deployed with virtual I/O identities.
Section	Displays the component that the attribute belongs to. For example, NIC.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute
Value	Displays the value of the attribute.

Related link


[Reclaim Identities Wizard](#)


Options

The **Options** page allows you to select your preferences for the reclaim identities task.

The fields displayed on the **Options** page of the **Reclaim Identities Wizard** are described in the following table.

Table 138. Options

Field	Description
Remove source from compute pool	<p>Select to move the server from the compute pool to the Repurpose and Bare Metal Devices group after reclaiming the identities of the server.</p> <p> NOTE: If this option is not selected, the server is retained within the compute pool after reclaiming the identities of the server.</p>
Force reclaim action even if target cannot be contacted	Select to reclaim the virtual I/O identities of the selected server, even if the server is unreachable.

Field	Description
	 NOTE: If the source server is not reachable and this option is: <ul style="list-style-type: none"> Not selected — The reclaim identities task is unsuccessful. Selected — The virtual I/O identities are reclaimed and available for use. However, you may notice devices with duplicate I/O identities on the network if the server is added back to the network.

Related link

[Reclaim Identities Wizard](#)

Credentials

The **Credentials** page allows you to provide the credentials of the selected server.

The fields displayed on the **Credentials** page of the **Reclaim Identities Wizard** are described in the following tables.

Table 139. Credentials

Field	Description
User Name	Provide the user name of the iDRAC of the server.
Password	Provide the password of the iDRAC of the server.

Related link

[Reclaim Identities Wizard](#)

Summary

The **Summary** page displays the options you have selected for the reclaim identities task.

The fields displayed on the **Summary** page of the **Reclaim Identities Wizard** are described in the following table.

Table 140. Summary


Field	Description
Name	Displays the name you have provided for the task.
Associated Devices	Displays the name of the device that you have selected for reclaiming the virtual I/O identities.
Remove from Pool	Displays if you have chosen to remove the server from the compute pool after reclaiming the virtual I/O identities.
Force reclaim identities	Displays if you have chosen to reclaim the virtual I/O identities of the server, even if the source server is unreachable.
Schedule	Displays the predefined task schedule.

Related link

[Reclaim Identities Wizard](#)

Managing device configuration baseline


The configuration of a server or chassis in a production environment must be properly maintained to ensure availability of the server. These server configuration settings tend to be drifted over time because of various reasons. The **Device Compliance Portal** enables you to verify and ensure the compliance of multiple servers and chassis to a device configuration baseline that serves as a baseline. The compliance status indicates if there is any difference between the current configuration settings and its corresponding baseline configuration. The **Device Compliance Portal** also allows you to create baselines, and assign the desired baseline to multiple production servers for establishing the compliance.

 **NOTE:** A device is considered to be compliant if it matches with all the settings defined in the associated baseline. A device with additional hardware (for example, an additional NIC card), is also considered to be compliant. A device may become non-compliant if there is a change in either the device inventory or the associated baseline. If the associated baseline is changed, the baseline must be redeployed to the associated devices.

 **NOTE:** Compliance tasks are not supported for IOA templates.

Using the **Device Compliance Portal**, you can:

- Create a configuration baseline from a server or chassis
- Associate a configuration baseline to a server or chassis
- View the tasks that have been created and their status
- Configure the deployment file share

 **NOTE:** The *device configuration deployment* and *configuration compliance* features are licensed (fee-based) for supported PowerEdge servers with iDRAC. To use these features on any PowerEdge VRTX or PowerEdge FX2/FX2s devices an Enterprise license is required. However, using it on PowerEdge M1000e devices does not require a license. Creating a device configuration baseline from a server does not require a license. For more information on licensing, see [OpenManage Essentials — Server Configuration Management License](#).

Related links

[Configuring the deployment file share](#)
[Creating a device deployment template](#)
[Configuring the credentials and device configuration inventory schedule](#)
[Associating target devices with a baseline](#)
[Viewing compliance status of devices](#)
[Viewing compliance tasks](#)
[Additional information](#)

Viewing the Device Compliance Portal

To view the device compliance portal, click **Manage** → **Configuration** → **Device Compliance Portal**.

Getting started for device configuration compliance

Before you can verify the compliance status of devices to a device configuration baseline, you must:

1. Configure the deployment file share on the server running OpenManage Essentials.
2. Configure the credentials and inventory schedule for target devices.

Related links

- [Configuring the deployment file share](#)
- [Configuring the credentials and device configuration inventory schedule](#)
- [Device configuration compliance overview](#)

Device configuration compliance overview

The steps that you must perform to verify the compliance status of a device and to make a device compliant to a device configuration baseline are as follows:

1. **Create a Baseline** — Use the **Create Baseline** task in the **Common Tasks** pane to create a device configuration baseline. You can choose to create the baseline from either a configuration file or a reference device.
2. **Associate Devices to a Baseline** — Select a baseline and associate it to applicable devices to view the compliance status.
3. **View the compliance status** — The **Device Compliance Portal** displays the compliance summary of all devices associated to the baselines. To view the compliance status of a device to an associated baseline, select the baseline in the **Baselines** pane. To view the detailed compliance results for each device, double-click the **Device Compliance** graph or table. Alternatively, you can also select the device in the device tree (**Manage** → **Devices**), and click the **Configuration** tab in the right-pane to view the compliance status.

Related link

- [Getting started for device configuration compliance](#)

Configuring the credentials and device configuration inventory schedule

The **Configuration Inventory Schedule** task enables you to collect an inventory of the device configuration attributes from applicable devices at periodic intervals. The inventory information is used to verify the compliance status of the devices to a specific device configuration baseline.

Before you configure the device inventory schedule, ensure that:

- The target devices meet the requirements that are specified in [Device Requirements for Deployment and Compliance Tasks](#).
- The Server Configuration Management license is installed on all target servers. For more information, see [OpenManage Essentials — Server Configuration Management License](#).

 **NOTE: Scheduled configuration inventory collection or update is not applicable for IOAs.**

To configure the device configuration inventory schedule:

1. Click **Manage** → **Configuration**.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Configuration Inventory Schedule**.
 - In the **Device Configuration Compliance Portal** pane, click **Getting Started for Compliance** → **Configure Credentials and Inventory Schedule for Target Devices**.

The **Configuration Inventory Schedule** wizard is displayed.

3. On the **Inventory Credentials** page:
 - a. Click **Add New Credential**.
The **Add Credentials** window is displayed.
 - b. Enter the description, username, and password.

 **NOTE: You must provide the iDRAC credentials that have Administrator rights.**

 **NOTE: The credentials can be edited at a later time only by the OpenManage Essentials user who added the credentials to the target devices.**

- c. If you want to set the credentials as the default credentials for all new target devices, select **Default**, and then click **Finish**.

- d. On the **Devices** section, set the **Execution Credentials** for each target device.
- e. Click **Next**.
4. On the **Schedule** page:
 - a. Select **Enable Configuration Inventory**.
 - b. If you want to run the configuration inventory immediately, select **Run Inventory on Finish**.
 - c. Select the desired scheduling parameters.
 - d. (Optional) You can adjust the **Inventory Polling Speed** slider for faster task execution; however, this consumes more system resources.
 - e. Click **Finish**.

The status of the task is displayed in **Task Execution History**. You can double-click the task in **Task Execution History** to view the task execution details.

Related links

[Server Configuration Management license](#)
[Device requirements for deployment and compliance tasks](#)
[Configuration Inventory Schedule Wizard](#)

Viewing the device configuration inventory

You can view the configuration inventory of a device through the **Devices** portal.

Before you begin, ensure that the device for which you want to view the configuration inventory, meets the requirements specified in [Device Requirements for Deployment and Compliance Tasks](#).

To view the configuration inventory:

1. Click **Manage** → **Devices**.
The **Devices** portal is displayed.
2. On the device tree, right-click the device for which you want to view the configuration inventory details, click **Device Configuration** → **Refresh Device Configuration Inventory**.
3. On the right pane, click **Configuration** → **Inventory**.
The inventory configuration details are displayed. If the inventory configuration task has not been run for the device, the **Run Configuration Inventory** button is displayed. You can click **Run Configuration Inventory** to view the configuration details, provided you have configured the credentials of the device in the **Inventory Configuration Schedule**.

Related link

[Device requirements for deployment and compliance tasks](#)

Creating a device compliance baseline for servers and chassis

You can create a device compliance baseline for a server or chassis that you have discovered.



NOTE: The chassis baseline does not include the IOA attributes.

To create a baseline for a server or chassis:

1. Click **Manage** → **Configuration**.
2. In the **Common Tasks** pane, click **Create Baseline**.
The **Create Baseline Wizard** is displayed.
3. In the **Name** field, enter a name for the baseline.
4. Select one of the following:
 - **Create from File:** To create a baseline by importing an XML template.
 - **Create from Device:** To create a baseline from a device.
5. Select the device type (Server, Chassis, or MX Chassis) and perform one of the following:
 - Select a device from the **All Applicable Devices** tree.
 - Search for a device by using the **Search Devices** box.

6. Under **Execution Credentials**, provide the device credentials that have the Administrator rights, and click **Finish**.
7. Click **Ok** in the task submission message.



NOTE: The destructive and password attributes information is not displayed while configuring a baseline. Only the non-destructive attribute information of the baseline is displayed.

Associating target devices with a baseline

The **Associate Devices to a Baseline** task enables you to designate the baseline to be used for verifying the compliance status of target devices.



NOTE: Before you begin to associate a configuration baseline to target devices, you must configure the credentials to run the device inventory. See [Configuring the credentials and device configuration inventory schedule](#).



NOTE: A device can only have one associated device configuration baseline. If you associate a second baseline to a device, the second baseline will become the only configuration baseline associated to the device.

To associate target devices to a baseline:

1. Click **Manage** → **Configurations**.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Associate Devices to a Baseline**.
 - In the **Compliance by Baseline** pane, either you right-click a baseline, and then click **Associate Devices**, or you click a baseline. The **Associate Devices** pop up wizard is displayed, and then click **Associate Devices**.
3. The **Associate Devices to a Baseline Wizard** is displayed.
4. On the **Select Baseline** page, select a server baseline, chassis baseline, or MX Chassis baseline from the list you want to associate with the target device, and then click **Next**.



NOTE: Only configuration baselines that you have either created or cloned are available for selection.

5. On the **Select Devices** page, select the target devices listed based on the baseline selected in step 4 from the **All Applicable Devices** tree, and then click **Finish**.

To view the updated compliance status of the devices, you must run the configuration inventory task. See [Viewing compliance status of devices](#).

Related links

[Baseline Association](#)

[Associate Devices To a Baseline Wizard](#)

Viewing compliance status of devices

Before you can view the compliance status of a device to an associated configuration baseline, you must run the device configuration inventory task. To run the device configuration inventory task, you can either create an inventory configuration schedule or select the device in the device tree and click **Run Configuration Inventory** on the **Configuration** tab in the right pane.



NOTE: Compliance tasks are not supported for IOA templates.

To view the compliance status of devices to the associated configuration baseline:




1. Click **Manage** → **Configurations** → **Device Compliance Portal**.
The **Device Compliance** graph and grid display the compliance status of the devices.
2. To view the devices by compliance status, click the **Device Compliance** graph.
3. To view the compliance status of a particular device, click the device in the **Device Compliance** grid.




NOTE: You can also select the device in the device tree (**Manage** → **Devices**), and click the **Configuration** tab in the right-pane to view the compliance status.

Remediating noncompliant devices

The devices which are not conforming to the associated baselines can be remediated to make them conform to the baseline configurations.

-  **NOTE:** The destructive and password attributes of the devices are not considered for compliance. As a result, these attributes are not considered for the remediation task.
-  **NOTE:** The user configuration attributes are successfully remediated only if the same user exists on the target devices. You cannot create a new user as the password attributes are not considered for remediation. For more details on creating an user, see [Deployment and reprovisioning](#).
-  **NOTE:** The remediation task fails for the devices which are noncompliant because of the missing attributes, or because of the dependency of attributes on other attributes that are not part of the compliance baseline. Clear the Deploy check box for the missing attributes in the corresponding baselines to make the devices compliant.

To remediate the devices which are not in compliance:

1. Click **Manage** → **Configuration** → **Make Device(s) Complaint**.
The **Name** page is displayed.
2. Enter the **Name** for the remediation task, and click **Next**.
3. On the **Select Devices** page, the list of noncompliant servers and chassis with the corresponding noncompliant attributes are displayed. Select all the noncompliant devices or the required devices from the list, and click **Next**.
4. On the **Options** page:
 - a. Select **Manual Server Reboot** to manually reboot the servers during the maintenance period. The compliance of the server is updated when the configuration inventory is refreshed as per the schedule or manually, post the reboot. The baselines that are associated with the chassis are deployed and the configuration changes are applied immediately.
 - b. Select **Automatic Server Reboot** to deploy the baselines that are associated with the selected devices immediately. If the configuration changes require the server to be rebooted, then a graceful shutdown is attempted first. If the graceful shutdown fails, then a force shutdown is carried out.
 -  **NOTE:** The chassis configurations are applied immediately and do not reboot the associated servers.
5. On the **Set Schedule** page:
 - a. Select either **Run now**, or click the calendar icon and select the date and time you want to run the task.
 - b. Under **Execution Credentials**, type the credentials of the selected device(s).
 - c. Click **Next**.
6. On the **Summary** page, review the information that you have provided, and then click **Finish**.
The remediation task is created and is run as per the selected schedule. You can double-click the task in **Task Execution History** to view the task execution details. The new attribute values that are assigned during the remediation task can be viewed in the **Details 1** tab.

The compliance of the devices is computed based on the remediation task result. To view the compliance status of the devices, see [Viewing compliance status of devices](#).

-  **NOTE:** In an MCM group, you can propagate the compliant attributes of the lead MX7000 chassis to the member chassis.

Viewing compliance tasks

To view the compliance tasks that have been created:

1. Click **Manage** → **Configuration**.
2. In the **Tasks** pane on the left, select a task type.
The **Task** tab on the right pane displays the tasks that have been created.

-  **NOTE:** Compliance tasks are not supported for IOA templates.

Related link

[Tasks](#)

Viewing server backup profiles

The server backup profile is created by scheduling a device configuration inventory. The device should be a part of the **Repurpose and Bare Metal Devices** group and should not be a part of the virtual I/O compute pool.

The backed-up profiles of the servers are visible under **Configuration Backup** → **Backed-up Devices**. Selecting one of the backed-up profiles under the **Devices** section, displays the attributes of the profile under the **Attributes** section. The attributes of the backed-up profiles are read-only and cannot be modified.

To replace a target server with the backup profile, see [Replacing a server from backup profile](#)

Replacing a server from backup profile

The replace server task allows you to replace a production server from the backup profile. When the replace server task runs, the attributes of the source server are migrated to the target server.

Before you begin to replace the target server, ensure that:

- The deployment file share is configured. For more information, see [Configuring the Deployment File Share](#).
- The credentials are configured and the configuration inventory of the devices is scheduled. See [Configuring the credentials and device configuration inventory schedule](#)
- The source and target devices are added to the **Repurpose and Bare Metal Devices** group. For more information, see [Adding Devices to the Repurpose and Bare Metal Devices Group](#).

To replace the target server from the backup profile:

1. Click **Replace Server** under **Manage** → **Configuration**.

Replace Server Wizard is displayed.



NOTE: To select an individual backup profile, in the **Devices** pane, right-click on the backed-up Device Name and select **Replace**.

2. Enter the task name, and click **Next**.
3. On the **Source and Target** page:
 - a. Under **Select Source**, select the source server.
 - b. Under **Select Target**, select the target server.
 - c. Click **Next**.

Note: The target server must be in the repurpose and bare metal group. To manually add the target server to the bare metal group, see [Adding Devices to the Repurpose and Bare Metal Devices Group](#).

4. In **Review Source Attributes**, the **Template Attributes**, the **Device Specific Attributes**, and the **Identity Attributes** are displayed. Click **Next**.



NOTE: The attributes displayed under **Review Source Attributes** are read-only.

5. On the **Options** page, select any of the following options based on your preference:
 - **Remove target from bare metal pool** — Select to remove the target server from the Repurpose and Bare Metal Devices group after the server is replaced.
 - Select **Deploy to target even if virtual identities cannot be removed from the source** to reclaim the virtual I/O identities of the source server, even if the source server is unreachable.
6. In the **Credentials** page, enter the **Source Credentials** and the **Target Credentials**. Click **Next**.

The **Summary** page is displayed.
7. The various attributes along with their values are listed in the **Summary** page. Review the selections you have made, and then click **Finish**.

The target server is replaced with the backup profile of the source server, and the replace server task is seen under **Tasks** → **Configuraton Tasks** → **Restore Server Configuration From Backup**. You can right-click the task in **Task Execution History** to

view the task execution details. The virtual identities reclaimed from the source devices are listed in the **Details 1** tab. The **Details 2** tab lists the attributes that are deployed on the target servers.



NOTE: If Remove target from bare metal pool option is selected, then the target server is removed from the Repurpose and Bare Metal Devices group.



NOTE: The target server is rediscovered, and the inventory details are updated for the target server.

Configuration – Reference

You can access the following from the **Manage** → **Configuration** page:

- Device Configuration Compliance Portal
 - Getting Started for Compliance — Displays the information required to setup, use, and get started with the device configuration compliance features.
 - Device Compliance Portal — Displays the default view of the **Device Compliance Portal**.
- Common Tasks — Displays the configuration compliance setup tasks and other tasks that you can create.
 - Create Baseline
 - Associate Devices to a Baseline
 - Make Device(s) Compliant
 - Configuration Inventory Schedule
 - File Share Settings
 - Replace Server
- Compliance by Baseline — Displays the sample device configuration baselines and the baselines that you have created or cloned.
 - Server Baselines
 - Samples
 - Chassis Baselines
 - Samples
 - MX Chassis Baselines
 - Samples
- Configuration Backup — Displays the backed-up devices which can be replaced with the target device.
 - Backed-Up Devices
- Tasks — Displays the tasks of the selected category in the **Tasks** tab in the right pane.
 - Configuration Tasks
 - MX Chassis Baseline Configuration Import — **Create Baseline** tasks you have created for MX7000 chassis.
 - Remediate Device Configuration — Remediation tasks of the non-complaint devices.
 - Replace Server Configuration From Backup — **Replace Server** tasks you have created for target devices.
 - Chassis Baseline Configuration Import — **Create Baseline** tasks you have created for chassis.
 - Device Baseline Configuration Import — **Create Baseline** tasks you have created for servers.



NOTE: For information on the sample device configuration templates, see the iDRAC documentation at [Dell.com/support](https://www.dell.com/support).

Related links

- [Device Compliance](#)
- [Tasks](#)
- [Task Execution History](#)
- [Associate Devices To a Baseline Wizard](#)
- [Configuration Inventory Schedule Wizard](#)
- [Backed-Up Devices](#)

Device Compliance

The **Device Compliance** graph and table enable you to view the compliance status of the devices.

Device Compliance Graph

The device compliance graph provides a pie chart distribution of the compliance status. Click a segment of the pie chart to view more information on the systems. The pie chart displays the following segments to indicate the device compliance status:

- Compliant — Devices that are compliant to the associated configuration baseline.
- Non Compliant — Devices that are not compliant to the associated configuration baseline.
- Non Inventoried — Devices on which configuration inventory is not completed.
- Non Associated — Devices that are not associated to a configuration baseline.
- Non Licensed — Devices that do not have the Server Configuration Management license installed.

Device Compliance Table

The fields displayed in the **Device Compliance** table of the **Device Compliance** portal are described in the following table.

Table 141. Device Compliance Table

Field	Description
Compliance Status	Displays an icon that indicates the compliance status of the device to the associated configuration baseline.
Device Name	Displays the unique name of the system that identifies it on the network.
Service Tag	Displays the unique identifier assigned to the system.
Model	Displays the model name of the system. For example, PowerEdge R710.
Compliance Template	Displays the device configuration template that is associated to the device.
Inventory Last Ran	Displays the date and time the last device configuration inventory was completed.

Tasks

The **Tasks** tab displays all the tasks that have been created.

The fields displayed in the **Tasks** tab of the **Device Compliance** portal are described in the following table.

Table 142. Tasks

Field	Description
Schedule	Displays if the task schedule is active or inactive.
Task Name	Displays the name of the task.
Type	Displays the type of task.
Description	Displays a brief description about the task.
Updated on	Displays the date and time the task was updated.
Updated by	Displays the name of the user who updated the task.
Created on	Displays the date and time the task was created.
Created by	Displays the name of the user who created the task.

Related link






[Viewing compliance tasks](#)

Task Execution History

The **Task Execution History** tab displays the status of tasks.

The fields displayed in the **Task Execution History** tab are described in the following table.

Table 143. Task Execution History

Field	Description
Status	Displays an icon representing the task status:  — Running or pending  — Complete  — Stopped  — Failed  — Warning
Task Name	Displays the name of the task.
Start Time	Displays the start time of the task.
% Completed	Displays the progress information of the task.
Task State	Displays the state of the task: <ul style="list-style-type: none"> Running Complete Stopped Failed Warning
End Time	Displays the end time of the task.
Executed by User	Displays the name of the user who executed the task.

Associate Devices To a Baseline Wizard

The **Associate Devices to a Baseline Wizard** enables you to associate devices to a baseline. The fields displayed in the **Associate Devices to a Baseline Wizard** are described in the following sections.

Related links

[Select Baseline](#)

[Select Devices](#)

[Associating target devices with a baseline](#)

Select Baseline

The **Select Baseline** page enables you to select the baseline you want to associate to target devices.

The fields displayed in the **Select Baseline** page are described in the following table.

Table 144. Select Baseline

Field	Description
Server Baselines	Displays the server configuration baselines that you have either created or cloned.
Chassis Baselines	Displays the chassis configuration baselines that you have either created or cloned.
MX Chassis Baselines	Displays the MX chassis configuration baselines that you have either created or cloned.

Select Devices

The **Select Devices** page enables you to select target devices to verify configuration compliance.

The **Select Devices** page displays the **All Applicable Devices** tree-view that includes the target devices. You can associate one or more target devices to a device configuration baseline.

Make Devices Compliant

The **Make Devices Compliant Wizard** enables you to remediate the non-compliant devices. The fields displayed in the **Make Devices Compliant Wizard** are described in the following sections.

Name

Table 145. Name

Field	Description
Name	Displays the name of the remediation task.

Select Devices



Table 146. Select Devices

Field	Description
Checkbox	Select a device or all the devices from the list of non-compliant devices.
Device Name	Displays the name of the device.
Service Tag	Displays the unique identifier assigned to the system.

Field	Description
Model	Displays the model name of the system. For example, PowerEdge R710.
Compliance Template	Displays the device configuration template that is associated to the device.
Inventory Last Run	Displays the date and time the last device configuration inventory was completed.
Non-Compliant Results	Displays the count of missing and non-compliant attributes.
Device Name	Displays the name of the device.
Compliance Result	Displays the compliance result of the device to the associated configuration baseline.
Component Name	Displays the name of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Template Value	Displays the template value of the attribute.
Inventory Value	Displays the inventory value of the attribute.

Options

Table 147. Options

Field	Description
Manual Server Reboot	<p>Select to manually reboot the server during the maintenance period. The baselines associated with the chassis are deployed and the configuration changes are applied immediately.</p> <p> NOTE: The configuration changes on the chassis will not result in the reboot of the servers associated with the particular chassis.</p>
Automatic Server Reboot	<p>Select to deploy the baselines associated with the devices immediately. If the configuration changes require the server to be rebooted, then a graceful shutdown is attempted first. If the graceful shutdown fails, then a force shutdown is carried out.</p> <p> NOTE: The configuration changes on the chassis will not result in the reboot of the servers associated with the particular chassis.</p>

Set Schedule

Table 148. Set Schedule

Field	Description
Run now	Select to run the remediation task immediately.
Run at	Select to schedule a task at a required date and time.
Execution Credentials	
User Name	Provide the user name configured on the device to run the task.
Password	Provide the password required to run the task.

Summary

Table 149. Summary

Field	Description
Name	Displays the name of the remediation task.
Non-Compliant Devices	Displays the selected non-compliant device name.
Reboot Option	Displays the selected reboot option.
Schedule	Displays the selected schedule to run the remediation task.

Configuration Inventory Schedule Wizard

The **Configuration Inventory Schedule** wizard enables you to associate the credentials to discovered devices and set the schedule for configuration inventory. The fields displayed in the pages of the wizard are described in the following sections.

Related links

[Inventory Credentials](#)

[Schedule](#)

[Configuring the credentials and device configuration inventory schedule](#)

Inventory Credentials

The **Inventory Credentials** page enables you to add credentials and associate credentials to target devices. The fields that are displayed in the **Inventory Credentials** page are described in the following table.

Credentials

The **Credentials** section displays a table that includes credentials that you have configured for the configuration inventory task.

Table 150. Credentials

Field	Description
Add New Credentials	Click to open the Add Credentials window that enables you to provide credentials for target devices.
Description	Displays the description that is provided for the credentials.
Username	Displays the username.
Password	Displays the password in a masked format.
Is Default	Displays a check box that you can select to associate the credentials to all new target devices.
Update	Displays an icon that you can click to edit the credentials.
Delete	Displays an icon that you can click to delete the credentials.
Created By	Displays the name of the user who provided the credentials.

Devices

The **Devices** section displays a table that includes the target devices for configuration compliance tasks.

Table 151. Devices

Field	Description
Device Name	Displays the Service Tag of the device.
Device Model	Displays the model name of the system, if available.


Field	Description
Execution Credentials	Displays the credentials that have been assigned to the device for running the configuration inventory task. You can use this field to assign the credentials that are required for running the configuration inventory task on the device.

Schedule

The **Schedule** page enables you to configure the schedule for the configuration inventory.

The fields displayed in the **Schedule** page are described in the following table.

Table 152. Schedule

Field	Description
Enable Configuration Inventory	Select to schedule configuration inventory.
Run Inventory on Finish	Select to run the configuration inventory after the inventory configuration is completed.
Configure Global Inventory Polling Interval	<p>Set the frequency of the inventory in weekly or daily intervals.</p> <p> NOTE: OpenManage Essentials performs configuration inventory only on devices that have already been discovered.</p> <ul style="list-style-type: none"> • Every Week On — Specify the day or days of the week that you want to schedule the inventory and the time that you want it to begin. • Every <n> Days <n> Hours interval — Specify the intervals between inventory cycles. The maximum discovery interval is 365 days and 23 hours.
Inventory Polling Speed	<p>Set the amount of resources available for accelerating the inventory poll speed. The faster you set the inventory poll speed, the more resources are required, but less time is required to perform the inventory.</p> <p>After changing the speed, OpenManage Essentials may take several minutes to adjust to the new speed.</p>

Backed-Up Devices

The **Backed-Up Devices** window displays the devices that are backed-up. The tables displayed in the **Backed-Up Devices** window are described in the following sections.

Devices Table

The fields displayed in the **Devices** table of the **Backed-Up Devices** portal are described in the following table.

Table 153. Devices Table

Field	Description
Connection Status	Displays the connection status of the device. The connection status are On or Off .
Health Status	Displays the health status of the device. The status options are Normal , Warning , Critical , and Unknown .
Device Name	Displays the unique name of the device that identifies it on the network.

Field	Description
Service Tag	Displays the unique identifier assigned to the device.
Model	Displays the model name of the device. For example, PowerEdge R730.
Last Backup Result	Displays the result of the last backup operation of the device.
Last Successful Backup Time	Displays the last successful backup time of the device.

Attributes Table

The fields displayed in the **Attributes** table of the **Backed-Up Devices** portal are described in the following table. The **Grouped By** filter can be used to display the table contents based on the filter option that is selected.

Table 154. Attributes Table

Field	Description
Section	Displays the component that the attribute belongs to. For example, iDRAC, BIOS, NIC, and so on.
Instance	Displays the instance of the component that the attribute belongs to.
Attribute Name	Displays the name of the attribute.
Value	Displays the value of the attribute.
Dependencies	Displays if the attribute is dependent on any other attributes. To edit a dependent attribute, you must first set the primary attribute.
Destructive	Displays if deploying the attribute may result in destructive changes to the device configuration including performance, connectivity, and ability to boot the device.
Group	Displays the group the attribute belongs to.

Viewing inventory reports

OpenManage Essentials provides pre-defined reports for all discovered and inventoried devices. With these reports, you can:

- Consolidate information about devices in your environment.
- Filter report data based on the devices by clicking the **Filter by:** drop-down list. You can also add a new group of devices from the dashboard by clicking **Add New Group** from the **Filter by:** drop-down list.
- Export data for use in another application in the XML file format.



NOTE: By default, the reports display the latest device information when you access the reports. If a report is open and you have not navigated from the report, you must click the refresh button to view the latest device information on the report.



NOTE: You cannot create new reports.

Choosing predefined reports

To view predefined reports, click **Reports**.

The **Managed Systems Reports** displays the predefined reports. Select from the available reports to view particular information about the devices in your environment. You can filter the reports based on the devices by clicking the **Filter by:** drop-down list. You can also add a new group of devices by clicking **Add New Group** from the **Filter by:** drop-down list.

Predefined reports

Table 155. Predefined reports

Category	Report	Description
Server Inventory	Agent and Alert Summary	<p>Identifies the OpenManage Server Administrator versions installed on devices in the environment and allows you to identify the devices generating the most alerts. If the Server Administrator is not installed on a server, it is displayed as None.</p> <ul style="list-style-type: none"> • The upper left web part identifies the OpenManage Server Administrator versions in your environment. • Clicking the OpenManage Server Administrator version in the OpenManage Server Administrator pie chart in the top right web part shows you the list of servers with that version installed. • The lower left web part lists in descending order the devices generating the most alerts since initial discovery and inventory. • The top five event generating devices are identified in the lower right web

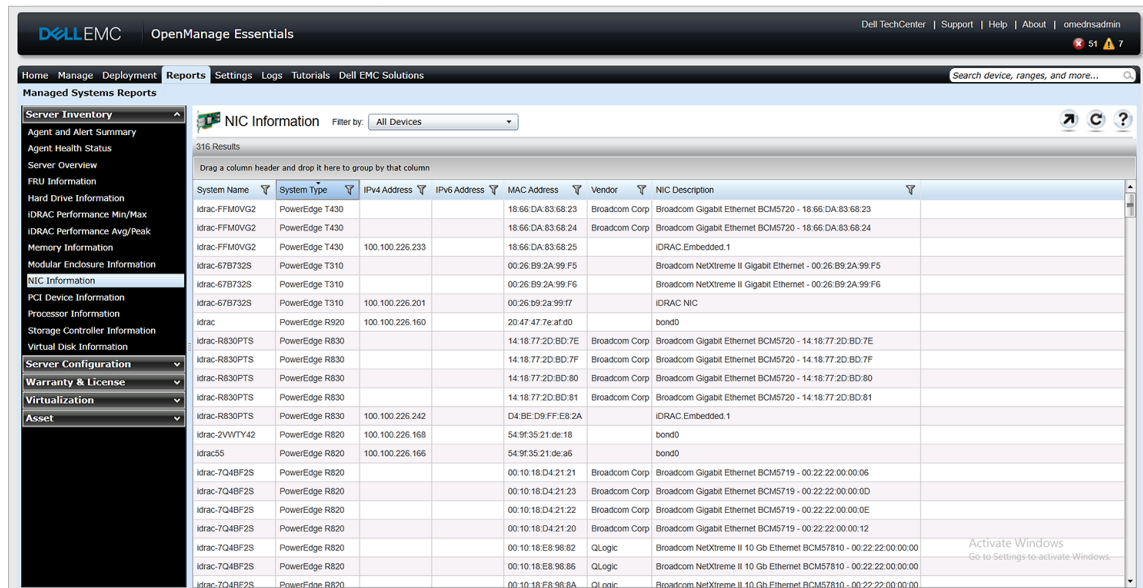
Category	Report	Description
		part. Click on a specific device to view the events associated with it.
	Agent Health Status	Provides information about the agent such as the system name, agent global status, agent name, and agent description.
	Server Overview	Provides information about the servers such as the system name, operating system installed on the server, processors, and memory.
	FRU Information	Provides details on replaceable server components.
	Hard Drive Information	Identifies serial number, revision, manufacturer, bus type, and self-encrypting capability for hard drives.
	iDRAC Performance Min/Max	Provides the minimum and maximum utilization of the processor, memory, and I/O bandwidth of a server.
	iDRAC Performance Avg/Peak	Provides the average and peak utilization of the processor, memory, and I/O bandwidth of a server.
	Memory Information	Provides details on DIMMs and identifies the slot a particular DIMM occupies within a server.
	Modular Enclosure Information	Provides information about the enclosure type, firmware version, enclosure Service Tag, and so on.
	NIC Information	Identifies the NIC model-IP address, MAC address, manufacturer and part and serial numbers for NICs.
	PCI Device Information	Identifies model, manufacturer, and slot for PCI and PCIe controllers in each server.
	Processor Information	Provides details about the processors in a server.
	Storage Controller Information	<p>Identifies the storage controllers on the server and provides the controller name, vendor, controller type, and controller state:</p> <ul style="list-style-type: none"> • Ready: The storage controller is ready for use. • Degraded: There is a potential problem with the controller. Investigation is required.

Category	Report	Description
	Virtual Disk Information	Provides information about the virtual disk such as size, layout, stripe size, and so on.
Server Configuration	Server Components and Versions	Identifies BIOS, driver, and firmware versions on all discovered and inventoried servers.
	BIOS Configuration	Provides the BIOS configuration information of the system.
	iDRAC Network Configuration	Provides IPMI over LAN, SSH, and Telnet status of the iDRAC.
	Device Configuration Compliance	Provides information about the compliance of a server or chassis to an associated device configuration template.
	Template Association	Provides information about the device configuration templates and the devices associated to the templates.
	Assigned Identity Attributes	Provides information about the virtual I/O identities that are assigned or deployed on a device and managed by OpenManage Essentials.
	All Identity Attributes	Provides information about all the virtual I/O identities that are present on a device and inventoried by OpenManage Essentials.
Warranty & License	Warranty Information	See Viewing Warranty Reports for details on how to run the warranty report and the information it provides.
	License Information	Provides the licensing information for the device.
Virtualization	ESX Information	Identifies ESX and ESXi virtual machine hosts and associated virtual machines.
	HyperV Information	Identifies the HyperV virtual machine hosts and associated virtual machines.
Asset	Asset Acquisition Information	Provides acquisition information about the devices.
	Asset Maintenance Information	Provides the maintenance information about the devices.
	Asset Support Information	Provides the support information about the devices.
	Device Location Information	Provides information about the location of a device in a data center.

Filtering report data

You can filter the results by dragging and dropping column headers to the top of reports. You can choose one or more attributes when revising the view to meet your specific needs.

For example, in the NIC Information report, drag the **System Type** and **System Name** to the top of the report. The view immediately changes to a nesting of information based on your preference. In this example, you can view nested data for NICs; NIC IP Address, MAC Address, and NIC description.



The screenshot shows the Dell OpenManage Essentials interface. The left sidebar contains a navigation menu with categories like Server Inventory, Agent and Alert Summary, FRU Information, Hard Drive Information, Memory Information, Modular Enclosure Information, NIC Information (selected), PCI Device Information, Processor Information, Storage Controller Information, Virtual Disk Information, Server Configuration, Warranty & License, Virtualization, and Asset. The main area displays the 'NIC Information' report with 316 results. A filter dropdown is set to 'All Devices'. A tooltip above the table indicates: 'Drag a column header and drop it here to group by that column'. The table has the following columns: System Name, System Type, IPv4 Address, IPv6 Address, MAC Address, Vendor, and NIC Description. The data rows show various network interface cards from vendors like Broadcom Corp and Intel, with details on their system names, types, addresses, and descriptions.

System Name	System Type	IPv4 Address	IPv6 Address	MAC Address	Vendor	NIC Description
idrac-FFM0VG2	PowerEdge T430			18:66:DA:83:68:23	Broadcom Corp	Broadcom Gigabit Ethernet BCM5720 - 18:66:DA:83:68:23
idrac-FFM0VG2	PowerEdge T430			18:66:DA:83:68:24	Broadcom Corp	Broadcom Gigabit Ethernet BCM5720 - 18:66:DA:83:68:24
idrac-FFM0VG2	PowerEdge T430	100.100.226.233		18:66:DA:83:68:25		IDRAC Embedded.1
idrac-67B732S	PowerEdge T310			00:26:B9:2A:99:F5	Broadcom NetXtreme II Gigabit Ethernet	00:26:B9:2A:99:F5
idrac-67B732S	PowerEdge T310			00:26:B9:2A:99:F6	Broadcom NetXtreme II Gigabit Ethernet	00:26:B9:2A:99:F6
idrac-67B732S	PowerEdge T310	100.100.226.201		00:26:B9:2A:99:F7		IDRAC NIC
idrac	PowerEdge R820	100.100.226.160		20:47:47:e:af:40		bond0
idrac-R830PTS	PowerEdge R830			14:18:77:2D:BD:7E	Broadcom Corp	Broadcom Gigabit Ethernet BCM5720 - 14:18:77:2D:BD:7E
idrac-R830PTS	PowerEdge R830			14:18:77:2D:BD:7F	Broadcom Corp	Broadcom Gigabit Ethernet BCM5720 - 14:18:77:2D:BD:7F
idrac-R830PTS	PowerEdge R830			14:18:77:2D:BD:80	Broadcom Corp	Broadcom Gigabit Ethernet BCM5720 - 14:18:77:2D:BD:80
idrac-R830PTS	PowerEdge R830			14:18:77:2D:BD:81	Broadcom Corp	Broadcom Gigabit Ethernet BCM5720 - 14:18:77:2D:BD:81
idrac-R830PTS	PowerEdge R830	100.100.226.242		D4:BE:D9:FF:E8:2A		IDRAC Embedded.1
idrac-2VW7Y42	PowerEdge R820	100.100.226.168		54:9F:35:21:de:18		bond0
idrac55	PowerEdge R820	100.100.226.166		54:9F:35:21:de:a6		bond0
idrac-7Q4BF2S	PowerEdge R820			00:10:18:D4:21:21	Broadcom Corp	Broadcom Gigabit Ethernet BCM5719 - 00:22:22:00:00:06
idrac-7Q4BF2S	PowerEdge R820			00:10:18:D4:21:23	Broadcom Corp	Broadcom Gigabit Ethernet BCM5720 - 00:22:22:00:00:00
idrac-7Q4BF2S	PowerEdge R820			00:10:18:D4:21:22	Broadcom Corp	Broadcom Gigabit Ethernet BCM5719 - 00:22:22:00:00:0E
idrac-7Q4BF2S	PowerEdge R820			00:10:18:D4:21:20	Broadcom Corp	Broadcom Gigabit Ethernet BCM5719 - 00:22:22:00:00:12
idrac-7Q4BF2S	PowerEdge R820			00:10:18:E8:98:82	QLogic	Broadcom NetXtreme II 10 Gb Ethernet BCM57810 - 00:22:22:00:00:00
idrac-7Q4BF2S	PowerEdge R820			00:10:18:E8:98:86	QLogic	Broadcom NetXtreme II 10 Gb Ethernet BCM57810 - 00:22:22:00:00:00
idrac-7Q4BF2S	PowerEdge R820			00:10:18:FA:98:8A	QLogic	Broadcom NetXtreme II 10 Gb Ethernet BCM57810 - 00:22:22:00:00:00

Figure 28. NIC Information Report

Exporting reports

Exporting a report enables you to manipulate and reformat the data. To export a report:

1. In the Reports list, right-click on any report to display the **Export** option.
2. Scroll over the **Export** option to display supported formats.
3. Choose your preferred format (CSV, HTML, or XML) and provide a file name for the exported report.

Reports — Reference

In the **Reports** portal, you can view various reports that are available under the following sections:

- **Server Inventory**
- **Server Configuration**
- **Warranty & License**
- **Virtualization**
- **Asset**

You can also filter the information based on a device or group by clicking **Filter by** and then selecting the device or group.

Related links

[Server Inventory Reports](#)

[Server Configuration Reports](#)

[Warranty and License Reports](#)

[Virtualization Reports](#)

[Asset Reports](#)

Server Inventory Reports

The **Server Inventory** section contains the following reports:

- **Agent and Alert Summary**
- **Agent Health Status**
- **Server Overview**
- **FRU Information**
- **Hard Drive Information**
- **iDRAC Performance Minimum/Maximum**
- **iDRAC Performance Average/Peak**
- **Memory Information**
- **Modular Enclosure Information**
- **NIC Information**
- **PCI Device Information**
- **Processor Information**
- **Storage Controller Information**
- **Virtual Disk Information**

Related links

[Agent and Alert Summary](#)
[Agent Health Status](#)
[Server Overview](#)
[Field Replaceable Unit Information](#)
[Hard Drive Information](#)
[iDRAC Performance Minimum or Maximum](#)
[iDRAC Performance Average or Peak](#)
[Memory Information](#)
[Modular Enclosure Information](#)
[NIC Information](#)
[PCI Device Information](#)
[Processor Information](#)
[Storage Controller Information](#)
[Virtual Disk Information](#)

Agent and Alert Summary

The **Agent and Alert Summary** displays the following:

- **Agent Summary**
- **iDRAC Service Module Summary**
- **Alerts per Device**
- **Top Alert Generators**

Agent Summary

The **Agent Summary** pane displays the agent summary information in a table and also as a chart.

Table 156. Agent Summary

Field	Description
Number of systems using specific Server Administrator agent	
Agent Details	Displays the name and version of the agent.
Number of systems utilizing this agent	Displays the number of systems utilizing a specific version of the agent.

iDRAC Service Module Summary

The **iDRAC Service Module Summary** pane displays the iDRAC Service Module summary information in a table and also as a chart.

Table 157. iDRAC Service Module Summary

Field	Description
Number of systems using specific iDRAC Service Module	
iDRAC Service Module Details	Displays the possibility of the iDRAC Service Module deployment on the discovered servers.
Number of systems	Displays the number of servers.

The **iDRAC Service Module Summary** chart displays the servers as:

- **Capable Linux** — The server does not meet some of the requirements for deploying iDRAC Service Module. For example, the server may not be running a 64-bit operating system or the version of the iDRAC firmware installed on the system may be prior to 1.51.51.
- **Deployable Linux** — iDRAC Service Module can be deployed on the server.

- Capable Windows — The server does not meet some of the requirements for deploying iDRAC Service Module. For example, the system may not be running a 64-bit operating system or the version of the iDRAC firmware installed on the system may be prior to 1.51.51.
- Deployable Windows — iDRAC Service Module can be deployed on the server.
- Incapable — iDRAC Service Module cannot be installed on the server. For example, the system may be a Dell 11th generation or earlier PowerEdge server.

Alerts per Device

Table 158. Alerts per Device

Field	Description
Most active discovered systems based on alert occurrence	
Device Name	Displays the unique name of the system that identifies it on the network.
Number of Associated Events	Displays the number of alerts from the device.
Last Discovered On	Displays the IP address range or host name.
Inventory Time	Displays the time and date information for the last run inventory.

Top Alert Generators

The **Top Alert Generators** pane displays the top five systems with the maximum alerts.

Agent Health Status

Table 159. Agent Health Status

Field	Description
System Name	Displays the host name of the system.
System Type	Displays the model name of the system.
Service Tag	Displays the unique identifier assigned to the system.
Agent Global Status	Displays the global health status of the agent.
Agent Name	Displays the name of the agent.
Agent Version	Displays the version of the agent.
Agent Description	Displays the agent details for the device.
Agent Manufacturer	Displays the name of the agent manufacturer.

Server Overview

Table 160. Server Overview

Field	Description
System Name	Displays the host name of the system.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Operating System	Displays the operating system installed on the system.
Processor Count	Displays the number of processors installed on the system.
Processor Family	Displays the type of processor installed on the system.

Field	Description
Processor Cores	Displays the number of processor cores.
Processor Speed	Displays the speed of the processor.
Total Cores	Displays the total number of cores present in the system.
Total Memory	Displays the total memory installed on the system

Field Replaceable Unit Information


Table 161. Field Replaceable Unit (FRU) Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
FRU Device Name	Displays the standard FRU name assigned to the device.
FRU Manufacturer	Displays the name of the FRU manufacturer.
FRU Serial Number	Displays the manufacturer specified identification number of the FRU.
FRU Part Number	Displays the industry specific number that differentiates the type of FRU.

Hard Drive Information

Table 162. Hard Drive Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Enclosure ID	Displays the enclosure ID assigned to the enclosure by Storage Management. Storage Management numbers the enclosures attached to the controller starting with zero.
Description	Displays the description of the media.
Channel	Displays the number of channels.
Target ID	Displays the SCSI ID of the backplane (internal to the server) or the enclosure to which the controller connector is attached. The value is usually 6.
LUN ID	Displays the LUN ID. In computer storage, a logical unit number or LUN number used to identify a logical unit, which is a device

Field	Description
	addressed by the SCSI protocol or similar protocols such as Fibre Channel or iSCSI.
Size (GB)	Displays the size of the hard drive in GB.
Bus Type	Displays the type of bus connection used. A bus, in computing, is an information pathway between components of a system.
Serial Number	Displays the roll number assigned to the device by the manufacturer.
Revision	Displays the revision history of the hard drive.
Media Type	Displays the type of media. For example, HDD.
Vendor	Displays the name of the organization that supplies the hard drive.
Model Number	Displays the model number of the physical device.
Part Number	Displays the unique number associated with a drives and drive capacity of a specific OEM vendor.
Remaining Rated Write Endurance	Displays the wear-out level or remaining life of the Solid State Drive (SSD) connected to a PERC in % units. If the drive does not support this property, it displays Not Applicable.
Supported Encryption Types	<p>Displays the list of hard drives that are encryption capable. It displays:</p> <ul style="list-style-type: none"> • Self Encrypting Drive (SED): If the hard drive is encryption capable. • None: If the drive is not encryption capable. • Not Available (N/A): If the data cannot be retrieved from the inventory. <p> NOTE: This feature is only available for iDRAC devices using WS-MAN protocol and OMSA devices using SNMP protocol.</p>

iDRAC Performance Minimum or Maximum

 **NOTE:** The iDRAC Performance Minimum/Maximum report provides information for Dell's 13th generation or later PowerEdge servers only.

Table 163. iDRAC Performance Minimum/Maximum

Field	Description
System Name	Displays the host name of the system.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Attribute	Displays the name of the performance attribute that is reported.
Last Hour (%)	Displays the usage level of the attribute in the last hour.

Field	Description
Last Hour Time Stamp	Displays the time at which the usage level was reported in the last hour.
Last Day (%)	Displays the usage level of the attribute in the last day.
Last Day Time Stamp	Displays the time at which the usage level was reported in the last day.
Last Week (%)	Displays the usage level of the attribute in the last week.
Last Week Time Stamp	Displays the time at which the usage level was reported in the last week.

iDRAC Performance Average or Peak

 **NOTE:** The iDRAC Performance Average/Peak report provides information for Dell's 13th generation or later PowerEdge servers only.

Table 164. iDRAC Performance Average/Peak

Field	Description
System Name	Displays the host name of the system.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Attribute	Displays the performance attribute that is reported.
Average Last Hour (%)	Displays the average usage level of the attribute in the last hour.
Average Last Day (%)	Displays the average usage level of the attribute in the last day.
Average Last Week (%)	Displays the average usage level of the attribute in the last week.
Peak Time Stamp	Displays the time at which the peak usage level was reported in the last week.

Memory Information

Table 165. Memory Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Name	Displays the name assigned to the device by the manufacturer. For example, DIMMI_A.
Size (MB)	Displays the size of the memory device in GB.
Memory Device Type	Displays the type of the memory device. For example, DDR3.

Field	Description
Memory Device Type Details	Displays details about the memory device type.
Memory Device Manufacturer	Displays the name of the device manufacturer.
Memory Device Part Number	Displays the industry specific number assigned to the device.
Memory Device Serial Number	Displays the roll number assigned to the device by the manufacturer.

Modular Enclosure Information

Table 166. Modular Enclosure Information

Field	Description
Enclosure Model Type	Displays the model name of the enclosure. For example, PowerEdge M1000e.
Slot	Displays the slot number on the enclosure.
Subslot	Displays the sub slot name.
Slot Name	Displays the slot name of the enclosure.
Slot Content	Displays whether the slot is available or occupied in the modular enclosure.
Firmware Version	Displays the firmware version installed on the enclosure.
Enclosure Service Tag	Displays the unique identifier assigned to the enclosure.
Enclosure Name	Displays the unique enclosure name that identifies it on the network.
Blade Model Type	The model name of the blade server. For example, PowerEdge M710.
Blade Service Tag	Displays the unique identifier assigned to the blade server.
Blade Host Name	Displays the host name of the blade server.
Blade OS	Displays the operating system installed on the blade server.

NIC Information

Table 167. NIC Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
IPv4 Address	Displays the unique IPv4 address assigned to the NIC device.
IPv6 Address	Displays the unique IPv6 address assigned to the NIC device.
MAC Address	Displays the unique Media Access Control address (MAC address) identifier assigned to network interfaces for communications on the physical network segment.

Field	Description
Vendor	Displays the name of the NIC supplier.
NIC Description	Displays information on the NIC device.

PCI Device Information

Table 168. PCI Device Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Device Card Description	Displays the type of Peripheral Component Interconnect card used. For example, 82546GB Gigabit Ethernet Controller.
Device Card Manufacturer	Displays the manufacturer information.
Device Card Slot Type	Displays the type of slot on the mother board into which the card is inserted.

Processor Information

Table 169. Processor Information

Field	Description
System Name	Displays the host name of the system.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Family	Displays the name of the processor family.
Speed (MHz)	Displays the speed of the processor in MHz.
Max Speed (MHz)	Displays the maximum speed of the processor in MHz.
Cores	Displays the number of cores in the processor.
Brand	Displays the name of the processor manufacturer.
Model	Displays the model information of the processor.
Stepping	Displays the version of the processor model.
Slot	Displays the slot occupied by the processor.
Status	Displays the status of the processor.

Storage Controller Information

Table 170. Storage Controller Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network. The storage controller is present on this system.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Controller Name	Displays the name of the storage controller. For example, SAS 6/iR Integrated.
Vendor	Displays the supplier information. For example, SAS 6/iR Integrated is supplied by Dell.
Controller Type	Displays the type of controller. For example, SAS 6/iR Integrated is of type SAS.
Controller State	Displays the state of the controller. For example, ready to use.

Virtual Disk Information

Table 171. Virtual Disk Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Target ID	Displays the SCSI ID of the backplane (internal to the server) or the enclosure to which the controller connector is attached.
Name	Displays the name of the virtual disk.
Device Name	Displays the name of the device on which the virtual disk is present.
Size (GB)	Displays the size of the virtual disk in GB.
Layout	Displays the RAID level.
Cache Policy	Displays the cache policy used for storage.
Read Policy	Displays the read policy used for storage.
Write Policy	Displays the write policy used for storage.
Strip Size (Bytes)	Displays the size of the stripe in bytes.

Server Configuration Reports

The **Server Configuration** section contains the following reports:

- **Server Components and Versions**

- BIOS Configuration
- iDRAC Network Configuration
- Device Configuration Compliance
- Template Association
- Assigned Identity Attributes
- All Identity Attributes

Related links

[Server Components and Versions](#)

[BIOS Configuration](#)

[iDRAC Network Configuration](#)

[Device Configuration Compliance](#)

[Baseline Association](#)

[Assigned Identity Attributes](#)

[All Identity Attributes](#)

Server Components and Versions

Table 172. Server Components and Versions

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Description	Displays the software information.
Software Type	Displays the type of software that is available on the system. For example, firmware.
Software Version	Displays the version number of the software that is available on the system.

BIOS Configuration

Table 173. BIOS Configuration

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Virtualization Technology	Displays whether the additional hardware capabilities provided by Virtualization Technology are enabled or disabled.
System Profile	Displays the selected system profile: Performance Per Watt (DAPC), Performance Per Watt (OS), Performance, Dense Configuration, or Custom.
User Accessible USB Ports	Displays the status of the User Accessible USB Ports option.

Field	Description
Cores per Processor	Displays the number of cores enabled in each processor.
Node Interleaving	Displays whether the Node Interleaving option is enabled or disabled.
Logical Processor	Displays whether the logical processor option is enabled or disabled.
Integrated RAID Controller	Displays whether the integrated RAID controller is enabled or disabled.
SR-IOV Global Enable	Displays whether the configuration of Single Root I/O Virtualization (SR-IOV) devices is enabled or disabled.
Execute Disable	Displays whether the execute disable memory protection technology is enabled or disabled.

iDRAC Network Configuration

Table 174. iDRAC Network Configuration

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
IPMI over Lan	Displays whether the IPMI over LAN interface option is enabled or disabled.
IPMI Community	Displays the SNMP community name for traps.
SSH	Displays whether SSH connection is enabled or disabled.
SSH Port	Displays the port number used by iDRAC for an SSH connection.
SSH Timeout	Displays the duration an SSH connection is allowed to remain idle.
Telnet	Displays whether Telnet connection is enabled or disabled.
Telnet Port	Displays the port number used by iDRAC for a Telnet connection.
Telnet Timeout	Displays the duration a Telnet connection is allowed to remain idle.

Device Configuration Compliance

Table 175. Device Configuration Compliance

Field	Description
Compliance Status	Displays the compliance status of the device to the associated configuration baseline.
Device Name	Displays the unique name of the system that identifies it on the network.
Service Tag	Displays the unique identifier assigned to the system.
Model	Displays the model name of the system. For example, PowerEdge R710.
Compliance Baseline	Displays the device configuration baseline that is associated to the device.
Inventory Last Ran	Displays the date and time the last device configuration inventory was completed.

Baseline Association

Table 176. Baseline Association

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Associated Baseline	Displays the device configuration baseline associated to the system.

Related link


[Associating target devices with a baseline](#)

Assigned Identity Attributes

Table 177. Assigned Identity Attributes

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Section	Displays the component to which the attribute belongs. For example, NIC, FC, and so on.

Field	Description
Instance	Displays the instance of the component to which the attribute belongs.
Attribute Name	Displays the name of the attribute.
Value	Displays the virtual I/O identity assigned or deployed on the system.
Compute Pool	Displays the name of the compute pool to which the device belongs.
Virtual I/O Pool	Displays the name of the virtual I/O pool from which the virtual I/O identity is assigned to the system.
Status	Displays if the system is deployed with virtual I/O identities.

 **NOTE:** The deployed state of the identity attributes may be redundant if there are duplicate identities generated by OpenManage Essentials in the network.

All Identity Attributes

Table 178. All Identity Attributes

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Section	Displays the component to which the attribute belongs. For example, NIC, FC, and so on.
Instance	Displays the instance of the component to which the attribute belongs.
Attribute Name	Displays the name of the attribute.
Value	Displays the virtual I/O identity assigned or deployed on the system.

Warranty and License Reports

The **Warranty & License** section contains the following reports:

- **Warranty Information**
- **License Information**

Related links

[Warranty Information](#)

[License Information](#)

Warranty Information

Table 179. Warranty Information

Field	Description
View and Renew Warranty	Displays a link you can click to open the Dell website from where you can view and renew the device warranty.
Device Name	Displays the unique name of the system that identifies it on the network. If applicable, the proxy settings must be configured to retrieve warranty data from Dell.com/support .
Model	Displays the model name of the system. For example, PowerEdge R710.
Device Type	Displays the type of device. For example, Server, Remote Access Controller, and so on.
Service Tag	Displays the unique identifier assigned to the system.
Service Level Code	Displays the service level code such as parts only warranty (POW), next business day onsite (NBD), and so on for a particular system.
Warranty Type	Displays the warranty type. For example, initial, extended, and so on.
Warranty Description	Displays the warranty details applicable for the device.
Service Provider	Displays the name of the organization that will provide the warranty service support for the device.
Shipped Date	Displays the date on which the device was sent from the factory.
Start Date	Displays the date from which the warranty is available.
End Date	Displays the date on which the warranty will expire.
Days Remaining	Displays the number of days the warranty is available for the device.

License Information

Table 180. License Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
Model Type	Displays the model name of the system. For example, PowerEdge R710.
License Description	Displays the level of features enabled in the license.
License Duration	Displays the duration of the license.
Entitlement ID	Displays the unique identifier for the license.
Time Remaining	Displays the days remaining until the license expires.

Virtualization Reports

The **Virtualization** section contains the following reports:

- **ESX Information**
- **HyperV Information**

Related links

[ESX Information](#)

[HyperV Information](#)

ESX Information

Table 181. ESX Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network. The embedded bare-metal product is installed on this system.
System Type	Displays the model name of the system. For example, PowerEdge R710.
VM Type	Displays the type of embedded bare-metal product installed on the system. For example, VMware ESX.
Version	Displays the version of the embedded bare-metal that is installed on the system.
Guest Name	Displays the name of the guest virtual machine.
Guest OS Type	Displays the operating system that is installed on the virtual machine.
Guest Memory Size (MB)	Displays the size of the RAM on the virtual machine.
Guest State	Displays whether the virtual machine is powered off or powered on.

HyperV Information

Table 182. HyperV Information

Field	Description
System Name	Displays the host name of the system on which the HyperV is installed.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Guest Name	Displays the name of the guest virtual machine.
Guest Memory Size (MB)	Displays the size of the RAM on the virtual machine.
Guest State	Displays whether the virtual machine is powered off or powered on.

Asset Reports

The **Asset** section contains the following reports:

- **Asset Acquisition Information**
- **Asset Maintenance Information**
- **Asset Support Information**
- **Device Location Information**

The reports in the **Asset** section depend on the following:

- The server must be discovered in-band with SNMP protocol.
- The asset information must be set in OMSA. To set the asset information in OMSA, go to **System** → **Properties** → **Asset Information**.

Related links

[Asset Acquisition Information](#)

[Asset Maintenance Information](#)

[Asset Support Information](#)

[Device Location Information](#)

Asset Acquisition Information

Table 183. Asset Acquisition Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Purchase Cost	Displays the price the owner paid for the system.
Purchase Date	Displays the date the owner purchased the system.
Way Bill Number	Displays the receipt from the carrier for the goods received.
Purchase Order Number	Displays the number of the document that authorized payment for the system.
Installation Date	Displays the date the system was put to service.
Expensed	Displays whether the system is charged to a specific purpose or department such as research and development or sales.
Cost Center	Displays the name or code for the business entity that acquired the system.
Signing Authority Name	Displays the name of the person who approved the purchase or the service call on the system.
Vendor	Displays the business entity that offers service on the system.
Depreciation Duration	Displays the number of years or months over which a system is depreciated.

Field	Description
Depreciation Duration Unit Type	Displays the unit in months or years.
Depreciation Percentage	Displays the portion of 100 that an asset is devalued or depreciated.
Depreciation Method	Displays the steps and assumptions used to compute the system's depreciation.
Ownership Code	Defines the ownership code for this system.
Corporate Owner Name	Displays the business entity that owns the system.
Insurance Company	Displays the name of the company that insures the system.

Asset Maintenance Information

Table 184. Asset Maintenance Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Multiple Schedules	Displays whether there are multiple schedules for the lease.
Buyout Amount	Displays the balance purchase price for the system.
Lease Rate Factor	Displays the rate factor for the lease on the system.
Lease End Date	Displays the end date for the lease on the system.
Fair Market Value	Displays the fair market value of the system.
Lessor	Displays the name of the lessor of the system.
Maintenance Provider	Displays the maintenance provider's name.
Maintenance Restrictions	Displays the maintenance agreement restrictions.
Maintenance Start Date	Displays the start date for maintenance on this system.
Maintenance End Date	Displays the end date for maintenance on this system.
Outsourcing Problem Description	Displays the problem encountered with the outsourcing service provider.
Outsourcing Service Fee	Displays the amount that the outsourcing vendor charges for service.
Outsourcing Provider Fee	Displays any additional outsourcing charge for service.
Outsourcing Provider Service Level	Displays the service level agreement for the system.
Outsourcing Signing Authority	Displays the name of the person who can sign the authorization for service.

Asset Support Information

Table 185. Asset Support Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Warranty Cost	Displays the extended warranty cost date for the system.
Warranty Duration	Displays the duration of the warranty.
Warranty Duration Type	Displays the warranty duration type for the system.
Warranty End Date	Displays the warranty end date for the system.
Extended Warranty Cost	Displays the cost of the warranty for the system.
Extended Warranty Start Date	Displays the extended warranty start date for the system.
Extended Warranty End Date	Displays the extended warranty end date for the system.
Extended Warranty Provider Name	Displays the name of the extended warranty provider for the system.
Contract Renewed	Displays whether the service contract for the system was renewed.
Contract Type	Displays the name of the service contract type for the system.
Contract Vendor	Displays the name of the service contract provider for the system.
Outsourced	Displays whether the support for the system is outsourced or not.
Support Type	Displays the type of component, system, or network problem that occurred.
Help Desk	Displays the help desk information provided
Automatic Fix	Displays the method used to fix the problem.

Device Location Information

Table 186. Device Location Information

Field	Description
System Name	Displays the unique name of the system that identifies it on the network.
System Type	Displays the model name of the system. For example, PowerEdge R710.
Service Tag	Displays the unique identifier assigned to the system.
Location	Displays the location of the system.

Field	Description
Data Center	Displays the data center where the system is available.
Room	Displays the name of the room where the system is available.
Aisle	Displays the aisle where the system is available.
Rack	Displays the rack where the system is available.

Viewing warranty reports

Warranty information is available for devices with valid Service Tags, including clients, servers, switches, storage, and so on. Warranty information is automatically retrieved at the time devices are discovered.

The Warranty Information report is unique among OpenManage Essentials reports as it requires Internet access to pull warranty information from the warranty database. If you do not have internet access, no warranty information is populated. It is downloaded the next time you connect to the internet and open the Warranty Report.



NOTE: The warranty information (including expired and renewed) displayed in OpenManage Essentials for a particular Service Tag, may not match with the warranty record displayed at Dell.com/support. The service level code and model name of a warranty record displayed at Dell.com/support may not exactly match with the OpenManage Essentials warranty report.

Extending warranty

To extend support for the devices, click **View and Renew Warranty** in the **Reports** → **Warranty Information** page. This opens the warranty site. You must log in to the warranty site with your company account to see all the devices and their warranty information.

Managing alerts

 **NOTE:** You can receive alert notifications from OpenManage Essentials on your Android or iOS device by installing and setting up the OpenManage Mobile application. For more information, see [OpenManage Mobile Settings](#) and the *OpenManage Mobile User's Guide* at Dell.com/OpenManageManuals.

With OpenManage Essentials you can:

- View alerts and alert categories
- Manage alert actions
- Configure alert log settings
- Manage MIB files
- Manage traps

Viewing alerts and alert categories

To view the alerts page, from OpenManage Essentials, click **Manage** → **Alerts**.






 **NOTE:** Alerts for deleted devices are not displayed in the console. However, these alerts are not deleted from the database until the purge limits are reached.

Viewing alert logs

To view alert logs, click **Manage** → **Alerts** → **Alert Logs**.

Understanding alert types

Table 187. Alert types

Icon	Alert	Description
 Figure 29. Normal alert icon	Normal Alerts	An event from a server or a device that describes the successful operation of a unit, such as a power supply turning on or a sensor reading returning to normal.
 Figure 30. Warning alert icon	Warning Alerts	An event that is not necessarily significant, but may indicate a possible future problem, such as crossing a warning threshold.
 Figure 31. Critical alert icon	Critical Alerts	A significant event that indicates actual or imminent loss of data or loss of function, such as crossing a failure threshold or a hardware failure.
 Figure 32. Unknown alert icon	Unknown Alerts	An event has occurred but there is insufficient information to classify it.
 Figure 33. Information alert icon	Information Alerts	Provides information only.

Viewing internal alerts

Before viewing internal alerts, ensure that you enable internal health alerts in the **Alert Settings** of the **Settings** tab. See [Alert Settings](#).

To view internal alerts, click **Manage** → **Alerts** → **Alert Logs** → **All Internal Alerts**.

The **All Internal Alerts** filter is a reference to the internal alerts that OpenManage Essentials generates when a change occurs in the global health or connection status of a managed device.

Viewing alert categories

To view alert categories, click **Manage** → **Alerts** → **Alert Categories**.

The predefined alert categories are listed in alphabetical order.

Viewing alert source details

To view an alert category, in the alert categories list, expand an alert category, and then select an alert source.

 **NOTE:** You cannot create a new event source.

For example, expand **Environmental** alert category and then select the **alertCoolingDeviceFailure** alert source.

Alert source values and descriptions for alertCoolingDeviceFailure

Table 188. Alert source values and descriptions for alertCoolingDeviceFailure

Field Name	Value	Description
Name	alertCoolingDeviceFailure	
Type	SNMP	An SNMP alert based source.
Catalog	MIB — 10892	
Severity	Critical	If this alert is received, then the system is in critical state and immediate action is required.
Format String	\$3	
SNMP Enterprise OID	.1.3.6.1.4.1.674.10892.1	
SNMP Generic Trap OID	6	
SNMP Specific Trap OID	1104	

Viewing previously configured alert actions

This section provides instructions to view previously configured alert actions.

Viewing application launch alert action

1. Select **Manage** → **Alerts** → **Alert Actions**.
2. In **Alert Actions**, select **Application Launch**.

Viewing email alert action

1. Select **Manage** → **Alerts** → **Alert Actions**.
2. In **Alert Actions**, select **Email**.

Viewing alert ignore action

1. Select **Manage** → **Alerts** → **Alert Actions**.
2. In **Alert Actions**, select **Ignore**.

Viewing alert trap forward action

1. Select **Manage** → **Alerts** → **Alert Actions**.
2. In **Alert Actions**, select **Trap Forwarding**.

Handling alerts

Flagging an alert

After you have completed action on an alert, flag the alert as acknowledged. Acknowledging an alert indicates it is resolved or does not require further action as a reminder to yourself. To acknowledge alerts:

1. Select **Manage** → **Alerts** → **Alert Logs**.
2. Click the alert you want to acknowledge.



NOTE: You can acknowledge multiple alerts simultaneously. Use <Ctrl> or <Shift> to select multiple alerts.

3. Right-click and click **Acknowledge** → **Set** → **Selected Alerts or Filtered Alerts**.

If you choose **Selected Alerts**, the highlighted alerts are acknowledged.

If you choose **Filtered Alerts**, all alerts in the current filter/view are acknowledged.

Creating and editing a new view

To personalize the way you view alerts, create a new view or modify an existing view. To create a new view:

1. Click **Manage** → **Alerts** → **Common Tasks** → **New Alert View Filter**.
2. In **Name and Severity Association**, enter a name for the new filter, and then check one or more severities. Click **Next**.
3. In **Categories and Sources Association**, assign the alert category or source to which you want to associate with this view filter and click **Next**.
4. In **Device Association**, create query for searching devices or assign the device or device groups, which you want to associate to this view filter and then click **Next**.
5. (Optional) By default the alert view filter is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next**.
6. (Optional) In **Acknowledged Association**, set duration when this alert action is active, and then click **Next**. The default is always active.
7. In **Summary**, review inputs and click **Finish**.

Configuring alert actions

Alert actions occur on all alerts received by the OpenManage Essentials console. The alert is received and processed by the OpenManage Essentials console whether or not OpenManage Essentials has discovered the device so long as OpenManage Essentials is listed in the device's SNMP trap forward destinations list. To prevent this, remove OpenManage Essentials from the SNMP trap forward destinations list on the device.

Setting up email notifications

You can create email notifications when an alert is received. For example, an email is sent if a critical temperature alert is received from a server.

To configure an email notification when alerts are received:

1. Select **Manage** → **Alerts** → **Common Tasks** → **New Alert Email Action**.
2. In **Name and Description**, provide email alert action name and description and then click **Next**.
3. In **E-mail Configuration**, do the following and then click **Next**.
 - a. Provide email information for the **To:** and **From:** recipients and provide the substitution information. Separate each recipient or distribution list with a semi-colon.
 - b. Customize the email message format with any of the following substitution parameters:
 - \$n = Device
 - \$ip = Device IP
 - \$m = Message
 - \$d = Date
 - \$t = Time
 - \$sev = Severity
 - \$st = Service Tag
 - \$r = Recommended Resolution
 - \$e = Enterprise OID
 - \$sp = Specific Trap OID
 - \$g = Generic Trap OID
 - \$cn = Alert Category Name
 - \$sn = Alert Source Name
 - \$pkn = Package Name
 - \$at = Asset Tag
 - \$loc = Device Location
 - \$mod = Model Name
 - c. Click **Email Settings** and provide SMTP server name or IP Address, to test email settings and click **OK**.
 - d. Click **Test Action** to send test email.
4. In **Severity Association**, assign the alert severity to which you want to associate this email alert and then click **Next**.
5. In **Categories and Sources Association**, assign the alert categories or alert sources to which you want to associate this email alert and then click **Next**.
6. In **Device Association**, assign the device or device groups to which you want to associate this email alert and then click **Next**.
7. By default the Email Notification is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next**.
8. In **Summary**, review the inputs and click **Finish**.

Related links

[Alert Logs](#)
[Alert Logs Fields](#)
[Alert Log Settings](#)
[Severity](#)

Ignoring alerts

Sometimes you will receive alerts you might want to ignore. For example, you may want to ignore multiple alerts generated when **Send authentication trap** is selected within the SNMP service on the managed node.

 **NOTE:** You can ignore all alerts from a particular device by using the **Ignore All Alerts from Device** option available when you right-click either a device on the device tree or an alert in the Alerts portal.

To ignore an alert:

1. From OpenManage Essentials, select **Manage** → **Alerts** → **Common Tasks** → **New Alert Ignore Action**.
2. In **Name and severity Association**, provide a name, assign the alert severity to which you want to associate this ignore alert action, and then click **Next**.

3. In **Categories and Sources Association**, assign the alert categories source to which you want to associate this alert ignore action and then click **Next**.
4. In **Device Association**, assign the device or device groups to which you want to associate this alert ignore action and then click **Next**.
5. By default the Ignore Alert is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next**.
6. In **Duplicate Alert Correlation**, select **yes** to exclude duplicate alerts received within the set time limit, and then click **Next**.
7. In **Summary**, review inputs and click **Finish**.

Running a custom script

In response to a specific alert received, you can run custom scripts or launch a specific application. This file must be present on the OpenManage Essentials service tier system (where OpenManage Essentials is installed) and not on the client browser system. For example:

- If you receive a temperature warning, you can use a custom script to create an incident ticket for your internal Help Desk.
- If you receive an MD Array storage alert, you can launch the Modular Disk Storage Manager (MDSM) application to view the status of the array.

Creating a custom script

1. Select **Manage → Alerts → Alert Actions**.
2. In **Alert Actions**, right-click **Application Launch** and select **New Alert Application Launch Action**.
3. In **Name and Description**, provide an application launch name and description and then click **Next**.
4. In **Application Launch Configuration**, provide an executable name (provide an absolute file path, for example, **C:\ProgramFiles\Dell\Application.exe**) and provide the substitution information, and then click **Next**.
5. In **Severity Association**, assign the alert severity to which you want to associate this alert application launch and then click **Next**.
6. In **Categories and Sources Association**, assign the alert categories or alert sources to which you want to associate this alert application launch and then click **Next**.
7. In **Device Association**, assign the device or device groups to which you want to associate this alert application launch and then click **Next**.
8. By default the Application Launch Action is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next**.
9. In **Summary**, review inputs and click **Finish**.

Related links

[Alert Logs](#)
[Alert Logs Fields](#)
[Alert Log Settings](#)
[Severity](#)

Forwarding alerts

You may want to consolidate alerts from multiple management stations to one management station. For example, you have management stations in multiple locations and you want to view status and take action from one central location. For information about the behavior of forwarded alerts, see [Forwarding Alerts Use Case](#).

To create alert forwards:

1. Select **Manage → Alerts → Common Tasks → New Alert Trap Forward Action**.
2. In **Name and Description**, provide Trap Forward name and description and then click **Next**.
3. In **Trap Forwarding Configuration**, provide destination host name or IP address, provide community information, to send a test trap to the destination management station, click **Test Action**. To forward the trap in the same format to the configured destination, click **Forward Trap in Original Format** and click **Next**.
4. In **Severity Association**, assign the alert severity to which you want to associate this trap forwarding alert and then click **Next**.
5. In **Categories and Sources Association**, assign the alert categories source to which you want to associate this trap forwarding alert and then click **Next**.

6. In **Device Association**, assign the device or device groups to which you want to associate this trap forwarding alert and then click **Next**.
7. By default the Trap Forward Action is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next**.
8. In **Summary**, review inputs and click **Finish**.
The severity status for any trap is set to normal and for a successful alert action, combination of severity, category, and device has to confer with the selections in the preceding steps.

Forwarding alerts use case scenarios

This section describes scenarios about forwarding alerts using the SNMP v1 and SNMP v2 protocols. The scenarios consists of the following components:

- Managed node with an SNMP v1 agent, referred to as MNv1
- Managed node with an SNMP v2/v2c agent, referred to as MNv2
- Managed station 1 with OpenManage Essentials, referred to as MS1
- Managed station 2 with OpenManage Essentials, referred to as MS2
- Managed station 3 with a third-party software, referred to as MS3

Scenario 1 — Forwarding Alerts in the Original Format Using SNMP v1 Protocol

In this scenario, SNMP v1 alerts are sent from MNv1 to MS1 and then forwarded from MS1 to MS2. If you try to retrieve the remote host of the forwarded alert, it displays the name of MNv1 as the alert originates from MNv1. MNv1 is displayed because the SNMP v1 alert standards allow you to set the agent name in the SNMP v1 alert.

Scenario 2 — Forwarding Alerts in the Original Format Using SNMP v2/v2c Protocol

In this scenario, SNMP v2 alerts are sent from MNv2 to MS1 and then forwarded from MS1 to MS3. If you try to retrieve the remote host of the forwarded alert from MS3, it is displayed as MS1

Since there are no fields in an SNMP v2 alert to specify the agent name, the host which sends the alert is assumed as the agent. When an SNMP v2 alert is forwarded from MS1 to MS3, MS1 is considered as the source of problem. To resolve this issue, while forwarding SNMP v2 or v2c alerts, a varbind is added with OID as .1.3.6.1.6.3.18.1.3.0 with the variable value as **Agent Address**. This has been set based on the standard OID specified in RFC2576-MIB. When you try to retrieve the **Agent Address** from MS3, it is displayed as MNv2

 **NOTE: If the SNMP v2 alert is forwarded from MS1 to MS2, the remote host is displayed as MNv2 because MS1 parses the extra OID along with the forwarded trap.**

Scenario 3 — Forwarding Alerts in the OMEssentials Format Using Either SNMP v1/v2 Protocol

In this scenario, SNMP v1 alerts are sent from MNv1 to MS1 and then forwarded to MS2. If you try to retrieve the remote host of the forwarded alert, it is displayed as MS1. The severity and the message of the alert is also defined by MS1 and does not display the original severity and message defined by MNv1.

 **NOTE: The same behavior applies for SNMPv2 traps.**

Working with sample alert action use cases

Sample alert actions are available for the **Application Launch**, **E-mail**, **Ignore**, and **Trap Forwarding** alert actions. Sample alert action use cases are disabled by default.

To enable a sample use case, right-click the use case and select **Enable**.

Use cases in alert actions

Application Launch

Sample - Run Script on Server Critical Alert—Enable this use case to run a custom script when a critical alert is received.

Email

- **Sample - Email Alerts to Service Desk**—Enable this use case to send an e-mail to the service desk account from the OpenManage Essentials server when an alert criteria is matched.
- **Sample - Email Critical Server Alerts to Admin**—Enable this use case to send an e-mail to an administrator from the OpenManage Essentials server when an alert criteria is matched.

Ignore

- **Sample - Ignore Alerts During Maintenance Window**—Enable this use case to ignore alerts during a specified time interval.
- **Sample - Ignore Duplicate Alerts with 15s**—Enable this use case to ignore duplicate alerts from the same system.
- **Sample - Ignore Non-Critical Alerts from Printers**—Enable this use case to ignore non-critical alerts related to printers.

Trap Forwarding

Sample - Forward Critical Server Alerts to Other Monitoring Console—Enable this use case to forward SNMP alerts another monitoring console.

Configuring alert log settings

You can configure alert log settings to set the maximum size of alert logs; to generate a warning alert when the alert log reaches a set threshold, and to purge the alert logs. To modify the default settings:

1. Select **Manage** → **Alerts** → **Common Tasks** → **Alert Log Settings**.

Alert Log Settings window is displayed.

2. Enter a value or use the increment/decrement arrow buttons to increase or decrease the value of the following fields:
 - a. **Maximum size of Alert Logs**
 - b. **Log a warning when the Alert Log size reaches**
 - c. **When the Alert Logs reach the Maximum size, purge**



NOTE: The default maximum size of alert logs is 40,000 alerts. Once that value is reached, the older alerts are purged.

3. Select **Save purged Alerts** to save the purged alert logs in .csv format.
4. Enter the **Purged Alerts Location**.
5. Click **Finish**.

The Alert Log Settings are configured and the specified Alert Logs are purged when the Maximum size is reached. The status of Alert Logs purging task is shown under **Logs** → **Application Logs**.

Renaming alert categories and alert sources

1. Click **Manage** → **Alerts** → **Alert Categories**.
2. In **Alert Categories**, right-click any of the alert categories (under the Alert Category heading in the left pane) and select **Rename**.
3. Provide a name for the alert category and click **OK**.

Alert pop-up notifications

The alert pop-up notification is displayed in the bottom-right corner of the OpenManage Essentials console when a **Critical** or **Warning** alert is received. The information displayed in the alert pop-up notification varies based on the number of alerts received.

If only one alert is received, the following information is displayed:

- Alert type — Warning or Critical.
- Name of the device that generated the alert.
- Alert description.
- **View Alert** — To view the Alert Details window.
- **Go to Device** — To navigate to the device in the device tree.
- **Disable** — To disable alert pop-up notifications.

If more than one alert is received, the following information is displayed:

- Alert type and frequency.
- Name of each device as a link to navigate to the device in the device tree.

 **NOTE: The device link is displayed only for the first three alerts.**

- **View Alerts** — To view the **All Recent Warning and Critical Alerts** window.
- **Go to Alert Console** — To navigate to the Alerts portal.
- **Disable** — To disable alert pop-up notifications.

By default, the alert pop-up notification is enabled. You can configure OpenManage Essentials to disable alert pop-up notifications or set the time interval between each alert pop-up notification.

 **NOTE: The Alert Pop-up Notification Settings is user-specific. The settings you have configured is not applicable to other users.**

Related links

[Configuring alert pop-up notifications](#)

[Enabling or disabling alert pop-up notifications](#)

Configuring alert pop-up notifications


1. Click **Settings** → **Alert Settings**.
The **Alert Settings** page is displayed.
2. Under **Alert Popup Notification Settings**, select or clear **Enable Alert Popup Notifications** to enable or disable alert pop-up notifications.
3. In the **seconds between popup notifications** box, select the time interval between each pop-up notification.
4. Click **Apply**.

Related link

[Alert pop-up notifications](#)

Enabling or disabling alert pop-up notifications

To enable or disable alert pop-up notifications:

 **NOTE: To quickly disable alert pop-up notifications, click the Disable link displayed in the alert pop-up notification. When the Disable Alert Popup Notifications prompt is displayed, click Yes.**

1. Click **Settings** → **Alert Settings**.
The **Alert Settings** page is displayed.
2. In **Alert Popup Notification Settings**:
 - Select the **Enable Alert Popup Notifications** option to enable alert pop-up notifications when a **Warning** or **Critical** alert is received.
 - Clear the **Enable Alert Popup Notifications** option to disable alert pop-up notifications.
3. Click **Apply**.

Related link

[Alert pop-up notifications](#)

Managing MIB files

OpenManage Essentials provides support for formatting hardware alerts (SNMP traps) for most enterprise devices. If you have non-Dell devices, you can use the **Alerts** portal to define new alerts for OpenManage Essentials. Defining alerts allows OpenManage Essentials to monitor a wider range of hardware and set up email and forwarding rules for these devices.

The **Alerts** portal allows you to extract trap definitions from SMIv1 or SMIv2 management information base (MIB) files. The extracted traps can be viewed and edited before importing them to OpenManage Essentials. This utility also allows you to manually

define and manage traps. Using the imported and manually-managed trap definitions, OpenManage Essentials properly classifies the incoming trap from a specific device.

 **NOTE: Importing traps portal is optional and only needed for formatting alerts from non-Dell devices.**

About importing MIBs

Use case scenario: As an administrator you want to monitor (listen and classify incoming traps) a device that is not supported by OpenManage Essentials.

Solution: Verify whether the device supports SNMP protocol. If the device supports SNMP protocol, ensure that the service is running and the trap destination points to the OpenManage Essentials-based system. For unsupported device traps, define the traps in OpenManage Essentials by importing the trap definitions using the **Alerts** portal. The following table provides information about traps before and after they are imported to the OpenManage Essentials database.

Table 189. Importing MIBs

Feature	Before Importing the MIB to the OpenManage Essentials Database	After Importing the MIB to the OpenManage Essentials Database
Can I see traps coming from the device in the OpenManage Essentials alerts portal?	Yes	Yes
Will traps have a severity value?	No, the severity is unknown.	Yes
Will traps have a valid name?	No, the name is unknown.	Yes, the trap name is defined in the MIB.
Will traps have a valid event category name?	No, the event category name is unknown.	Yes, a new category is created by default.
Will traps have a description?	Yes, all the description details are present. However, the details are not formatted.	Yes, the description is present in the format defined while importing the trap.
Will the trap display the trap variable values?	Yes	Yes (by default), provided the format string values are not removed prior to importing the traps to OpenManage Essentials.
Will the trap display the Enterprise object identifier (OID), Specific OID, and Generic OID?	Yes	Yes
Will the trap display additional trap variables which can be used for debugging?	Yes, however, the details are not formatted.	Yes
Will the trap display the host name or IP address of the device?	Yes	Yes
Can I use traps in various alert actions to forward the trap to another management console, execute a task, or filter the unwanted traps?	Yes, but the features are limited. Rules specific to severity, event category, event name, and so on are not possible.	Yes, the traps are defined so all the alert actions are supported based on the trap name, category, severity, and so on.
Can I perform various UI actions (acknowledge, delete, and so on) on the traps?	Yes	Yes
Will purging of alerts work on the traps?	Yes	No

Importing MIBs

Before you begin, ensure that you are logged in with OmeAdministrator privileges.

1. Click **Manage** → **Alerts** → **Manage MIBs**.
2. In **Manage MIBs**, click **Import MIB**.
3. In **Select files for upload**, click **Browse**.
 - a. Select the MIB files that you want to import.
 - b. Click **Open**.
4. From the **Select a MIB File** list, select a MIB file and then click **Parse MIB**.

The trap data appears in a grid format.
5. Click **Import Traps** to import traps into the OpenManage Essentials database.

Removing MIBs from OpenManage Essentials

Removing MIBs from OpenManage Essentials impacts the associated alert actions and existing alerts in the console. Before you begin, ensure that you are logged in with OmeAdministrator privileges.

1. Click **Manage** → **Alerts** → **Manage MIBs**.
2. In **Manage MIBs**, click **Remove MIB**.
3. Select the MIBs in the **Imported MIBs**.
4. Click **Remove MIB**.

Managing traps

Customizing trap definitions

The **Custom Trap Definitions** view enables you to add trap definitions to the OpenManage Essentials database. You can add a new trap definition or search unknown traps received in OpenManage Essentials, define the trap details and add the trap.

 **NOTE:** When you use the **Unknown Traps** button to add unknown traps received in OpenManage Essentials, the **Enterprise OID**, **Generic ID** and **Specific ID** fields are automatically populated.

Before you begin, ensure that you are logged in with OmeAdministrator privileges.

To add traps:

1. Click **Manage** → **Alerts** → **Manage Traps**.
2. In **Manage Traps**, click **Custom Trap Definitions**.

The **Custom Trap Definitions** view is displayed.
3. If you want to add a new trap definition:
 - a. In the **Category Name** list, select an existing category or type a new category name.
 - b. Provide the **Trap Name**, **Description**, **Enterprise OID**, **Specific ID**, and **Format String**.
 - c. In the **Severity** list, select a severity level for the trap.
4. If you want to add an unknown trap received in OpenManage Essentials:
 - a. Click **Search Unknown Traps**.

The **Unknown Traps in OpenManage Essentials** window is displayed.
 - b. Select an unknown trap you want to define and add and click **OK**.

The **Enterprise OID**, **Generic ID** and **Specific ID** fields are populated automatically based on the selected unknown trap.
 - c. In the **Category Name** list, select either an existing category or type a new category name.
 - d. Provide the **Trap Name**, **Description**, and **Format String**.
 - e. In the **Severity** list, select a severity level for the trap.
5. Click **Add Trap**.

The trap details you provided are displayed in the **User-defined Traps** grid.

Deleting traps

The **Custom Trap Definitions** view also enables you to delete user-defined traps. Traps that are pre-defined in OpenManage Essentials cannot be deleted.

Before you begin, ensure that you are logged in with OmeAdministrator privileges.

To delete traps:

1. Click **Manage** → **Alerts** → **Manage Traps**.
2. In **Manage Traps**, click **Custom Trap Definitions**.
3. In the **User Defined Traps** grid, select the traps you want to delete.
The selected traps are highlighted.
4. Click **Delete Trap**.
The confirmation dialog box is displayed.
5. Click **Yes**.

Resetting built-in trap definitions

The **Reset Built-in Trap Definitions** view enables you to reset a pre-defined OpenManage Essentials trap that you edited earlier.

Before you begin, ensure that you are logged in with OmeAdministrator privileges.

To revert traps:

1. Click **Manage** → **Alerts** → **Manage Traps**.
2. In **Manage Traps**, click **Reset Built-in Trap Definitions**.
The **Revert Trap** view displays all the pre-defined trap definitions that you edited.
3. In the **Edited Traps** grid, select the traps you want to revert and click **Revert Traps**.
The confirmation dialog box is displayed.
4. Click **Yes**.

Configuring SNMPv3 traps

The latest version of OpenManage Essentials supports SNMPv3 traps. The SNMPv3 traps offer enhanced security than V1/V2c notifications. The Windows trap service is disabled when SNMPv3 traps is selected. For more information, see [Alert Settings](#).

To configure SNMPv3 traps:

1. Select **Manage** → **Alerts** → **Common Tasks** → **SNMP V3 Trap Configuration**.

SNMP V3 Trap Configuration window is displayed.



NOTE: The SNMPv3 trap configuration details are automatically populated for the devices discovered using the SNMPv3 protocol. To receive the SNMPv3 traps, enable SNMPv3 trap listener under Settings → Alert Settings.

2. Enter the details in the following columns for the devices discovered using SNMP V1/V2c or WSMAN protocols:



NOTE: The details in the SNMP V3 Trap Configuration window can be edited only if Support V1/V2c/V3 Traps is selected under Alert Settings → SNMP Listener Settings. If Support V1/V2c is selected, then you can view the details only.

- a. Username
 - b. Authentication Protocol
 - c. Authentication Password
 - d. Encryption Protocol
 - e. Encryption Password
3. To configure the SNMPv3 trap manually:
 - a. Click **Add New**.
SNMP V3 Trap Configuration window is displayed.
 - b. Enter the details in the following fields:

- Agent IP Address
 - Engine ID
 - Username
- c. Select the **Authentication Protocol** from the list.

 **NOTE: SHA1 is the authentication protocol selected by default.**

- d. Enter the **Authentication Password**.
- e. Select the **Encryption Protocol** from the list.

 **NOTE: AES is the encryption protocol selected by default.**

 **NOTE: If the Authentication Protocol is set to None, then the authentication and encryption options are disabled.**

- f. Click **OK**.

The configured SNMPv3 trap profile is displayed in the **SNMP V3 Trap Configuration** window.

4. Alternatively, to import the .csv file containing the credentials:

- a. Click **Export** to generate a sample .csv file.
- b. Save the file to your system, and populate the Agent IP Address, Engine ID, Username, Authentication Protocol, Authentication Password, Encryption Protocol, and Encryption Password fields in the .csv file.
- c. Click **Import** to import the .csv file.

The imported credentials are displayed in the **SNMP V3 Trap Configuration** window.

Alerts — Reference

This page provides the following information:

- Common Tasks
 - Alert Log Settings
 - New Alert View Filter
 - New Alert Application Launch Action
 - New Alert Email Action
 - New Alert Ignore Action
 - New Alert Trap Forward Action
 - SNMP V3 Trap Configuration
- Alert Logs
 - Alert View Filters
 - All Alerts
 - All Internal Alerts
 - Critical Alerts
 - Info Alerts
 - Normal Alerts
 - Unknown Alerts
 - Warning Alerts
- Alert Actions
 - Application Launch
 - E-mail
 - Ignore
 - Trap Forwarding
- Alert Categories
- Manage MIBs
- Manage Traps

Alert Logs

You can view alerts from **Alerts Logs**. The Alert Logs allow you to view all alerts filtered by the active view filter. The criteria for matching the alerts in the view filter include:

- Alert severity. See [Severity](#).
- Alert category or source. See [Category and Sources Association](#).
- Alert device or device group source. See [Device Association](#).
- Alert date, time, or day of week. See [Date and Time Range](#).
- Alert acknowledged flag. See [Acknowledgement](#).

Related links

[Configuring alert log settings](#)
[Configuring alert actions](#)
[Setting up email notifications](#)
[Creating a custom script](#)
[Alert Logs Fields](#)
[Alert Log Settings](#)
[Severity](#)

Predefined Alert View Filters

The following table lists the predefined alert view filters.

Table 190. Predefined Alert View Filters

Field	Description
All Alerts	Select to view all the alerts.
Critical Alerts	Select to view all the systems that are critical.
Info Alerts	Select to view informational alerts.
Normal Alerts	Select to view normal alerts.
Unknown Alerts	Select to view alerts that OpenManage Essentials cannot categorize.
Warning Alerts	Select to view all the warnings.

Select **Continuous Updates** to enable the user interface to update automatically when new alerts are received.

Alert Logs Fields

Table 191. Alert Logs Fields

Field	Description
Severity	The alert severity
Acknowledged	Whether the alert has been acknowledged or not by the user.
Time	The date and time the alert was generated.
Device	The device which generated the alert.
Details	The message contained in the alert.
Category	The categorization of the alert.
Source	The name of the alert source definition.

Group By Column


To group by in **All Alerts**, drag the All Alert column that you want to group by and drop it in **Drag a column header and drop it here to group by that column**.

For example, In **All Alerts**, if you want to group by severity, select **Severity** and drag and drop it in the **Drag a column header and drop it here to group by that column** bar.

The alerts are displayed by severity.

Alert Details

Table 192. Alert Details

Field	Description
Severity	The alert severity.
Acknowledged	Whether the alert has been acknowledged or not by the user.
Recommended Resolution	<p>Click to view the recommended resolution for the issue that resulted in the alert.</p> <p> NOTE: The recommended resolution is available only for alerts received from either OMSA installed on the server or the iDRAC of the server. Alerts received from OMSA include the recommended resolution only if the Enhanced Message Format option is enabled in OMSA.</p>
Device	The device which generated the alert.
Time	The date and time the alert was generated.
Category	The categorization of the alert.
Source	The name of the alert source definition.
Description	The message contained in the alert.
SNMP Enterprise OID	Provides the enterprise OID (SNMP OID prefix) of the management information base (MIB) file that defines the event source that you want to monitor.
SNMP Generic Trap OID	Provides the generic trap ID of the SNMP trap that you want to monitor from the desired event source. See the <i>Dell OpenManage Server Administrator SNMP Reference Guide</i> at Dell.com/OpenManageManuals for more information on SNMP traps.
SNMP Specific Trap OID	Provides the specific trap ID of the SNMP trap that you want to monitor from the desired event source. See the <i>Dell OpenManage Server Administrator SNMP Reference Guide</i> at Dell.com/OpenManageManuals for more information on SNMP traps.

Alert Log Settings

Configure settings which control the size, messaging, and purge settings of the Alert Logs.

Table 193. Alert Log Settings

Field	Description
Maximum size of Alert Logs	Determines the maximum number of alerts the alert logs can have before purging occurs.
Log a warning when the Alert Log size reaches	A warning alert is sent to the application log when this size is reached.
When the Alert Logs reach the Maximum size, purge	Purges the specified number of alerts when the maximum size is reached.

Field	Description
Save Purged Alerts	If selected, the specified number of alerts are purged and saved in a .csv file.
Purged Alerts Location	Specifies the location where the purged alerts are saved as a .csv file.

Alert View Filters

 **NOTE:** You can receive alert notifications from OpenManage Essentials on your Android or iOS device by installing and setting up the OpenManage Mobile application. For more information, see [OpenManage Mobile Settings](#) and the *Dell OpenManage Mobile User's Guide* at Dell.com/OpenManageManuals.

Alert Filter Name

In OpenManage Essentials, you use alert filters that are associated with alert actions to implement alerting capabilities. For example:

- You can create alert action associations to trigger actions, such as sending e-mails, when an alert condition is met.
- You can create ignore, exclude, or both associations to ignore SNMP traps and CIM indications when they are received. You use these associations to suppress alert floods.
- You can create alert view filters to customize the **Alert Logs** view.

For more information about creating alert action associations, see [Managing Alerts](#).

Use this window to perform the following tasks:

- Create new alert action associations, ignore/exclude filters, and alert view associations.
- View summary information for alert action associations, ignore/exclude associations, and alert view filters.
- Edit, delete, rename, and copy alert action associations, ignore/exclude associations, and alert view filters.

Severity

This page provides a list of alert severity.

Table 194. Severity

Field	Description
Name	Name of the item (applicable only for ignore action and view filter).
Enabled	Select to enable the alert action (applicable only for ignore action).
Severity	The available alert types.
All	Select to include all types of alerts.
Unknown	Select to include unknown alerts.
Info	Select to include informational alerts.
Normal	Select to include normal alerts.
Warning	Select to include warning alerts.
Critical	Select to include critical alerts.

Acknowledgement

Table 195. Acknowledgement

Field	Description
Limit alerts based on the acknowledge flag	Select to configure the alert view filter to display alerts based on whether the alerts have been acknowledged or not. This option is disabled by default.
Match only acknowledged alerts	Select to display acknowledged alerts.
Match only unacknowledged alerts	Select to display unacknowledged alerts.

Summary — Alert View Filter

The **Summary** page is shown on the final page of the **Alert View Filter** wizard or when clicking the **View Summary** right-click option in the tree.

Table 196. Alert View Filter

Field	Description
Name	The name of the alert action.
Type	The alert action type — App Launch, Email, Ignore, Trap, and Forward.
Description	The description of the alert action.
Associated Severity	The alert severity criteria used when matching alerts.
Associated Alert Categories	The alert category criteria used when matching alerts.
Associated Alert Sources	The alert source criteria used when matching alerts.
Associated Device Groups	The alert source device group criteria used when matching alerts.
Associated Devices	The alert source device criteria used when matching alerts.
Associated Date Range	The alert date range criteria used when matching alerts.
Associated Time Range	The alert time range criteria used when matching alerts.
Associated Days	The alert days criteria used when matching alerts.
Associate Acknowledge	If enabled, uses the alert acknowledged flag when matching alerts.

Alert Actions

Alert actions are triggered when an incoming alert matches the specific criteria defined in the alert action. The criteria for matching the alert include:

- Alert severity. See [Severity Association](#).
- Alert category or source. See [Category and Sources Association](#).
- Alert device or device group source. See [Device Association](#).
- Alert date, time, or day of week. See [Date and Time Range](#).

There are four types of alert actions:

- **Alert Application Launch Action** — Launch a script or batch file when the alert action criteria is matched.
- **Alert Email Action** — Send an e-mail when the alert action criteria is matched.
- **Alert Ignore Action** — Ignore the alert when the alert action criteria is matched.

- **Alert Trap Forward Action** — Forward the SNMP Trap to another management console when the alert action criteria is matched.

By default, new alert actions are enabled. If you want to turn off the alert action without deleting it, you can disable it either through the right-click menu or the edit wizard for the alert action.

Several common alert action use cases are pre-installed in the disabled state to illustrate common usage. When using these pre-installed actions, it is recommended to clone the example to a new action specific to your needs. Make sure to enable and test the new action during this process.

Name and Description

Table 197. Name and Description

Field	Description
Name	The name of the alert action.
Description	The description of the e-mail action.
Enabled	Select to activate the alert action.

Severity Association

Table 198. Severity Association

Field	Description
Severity	The available alert types.
All	Select to include all types of alerts.
Unknown	Select to include unknown alerts.
Info	Select to include informational alerts.
Normal	Select to include normal alerts.
Warning	Select to include warning alerts.
Critical	Select to include critical alerts.


Application Launch Configuration


Use this window to configure the application that you want to launch and to test the launch.

 **NOTE:** Alert actions are run when a matching alert is received so the alert application launch action is a script or batch file that does not require user interaction.

Table 199. Application Launch Configuration

Field	Description
Executable Name	Specifies the fully qualified path name and file name of the executable file that launches the application program.
Arguments	<p>Specifies or edits any required or desired command line parameters to be used in launching the application program. You can use the following variable substitutions to specify information in the Arguments field:</p> <ul style="list-style-type: none"> • \$n = Device • \$ip = Device IP • \$m = Message • \$d = Date • \$t = Time

Field	Description
	<ul style="list-style-type: none"> • \$sev = Severity • \$st = Service Tag • \$r = Recommended Resolution • \$e = Enterprise OID • \$sp = Specific trap ID • \$g = Generic trap ID • \$cn = Alert Category Name • \$sn = Alert Source Name • \$pkn = Package Name • \$at = Asset Tag • \$loc = Device Location • \$mod = Model Name <p>Executable file: If you have an executable file (for example, createTroubleTicket.exe), to create a trouble ticket with parameters –arg1, –arg2, and so on; configure the alert application launch as follows:</p> <ul style="list-style-type: none"> • Executable Name (with the full path): C:\temp\createTroubleTicket.exe • Argument: –arg1 –arg2 <p>When the alert action is triggered, it runs the command C:\temp\createTroubleTicket.exe –arg1 –arg2 to perform the associated application launch alert action.</p> <p>Batch file: If you have a batch file (for example, createTroubleTicket.bat), to create a trouble ticket with parameters –arg1, –arg2, and so on, configure the alert application launch as follows:</p> <ul style="list-style-type: none"> • Executable Name (with the full path): C:\temp\createTroubleTicket.bat • Argument: –arg1 –arg2 <p>When the alert action is triggered, it runs the command C:\temp\createTroubleTicket.bat –arg1 –arg2 to perform the associated application launch alert action.</p> <p>VB script: When configuring vb script files as an alert action, provide the executable and arguments as follows. For example, if you have a script (createTroubleTicket.vbs), to create a trouble ticket that contains one parameter arg1, configure the application launch as follows:</p> <ul style="list-style-type: none"> • Executable Name: cscript.exe or C:\Windows\System32\cscript.exe (full path) • Argument: C:\temp\createTroubleTicket.vbs arg1 <p>When the alert action is triggered, it runs the command cscript.exe C:\temp\ createTroubleTicket.vbs arg1 to perform the associated application launch alert action.</p> <p> NOTE: If an alert action is not working, ensure that you have entered complete command from the command prompt.</p> <p>See the sample alert action under Application Launch alert action for more information.</p>
Test Action	Allows you to test the application launch.


Field	Description
	 NOTE: Alert actions are run when a matching alert is received; so the alert application launch action is a script or batch file that does not require user interaction.

E-Mail Configuration

You can configure Essentials so that you receive e-mail each time the alert associations for your devices meet specific alert criteria. For example, you may want to receive an e-mail message for all warning and critical alerts.

Use this window to specify the parameters for configuring the e-mail alert action.

Table 200. E-Mail Configuration

Field	Description
To	Specifies a valid e-mail address served by the company's SMTP server of the person who is to receive the e-mail.
From	Specifies the originating e-mail address.
Subject	Specify the e-mail subject using text or the available alert tokens.
Message	Specify the e-mail message using text or the available alert tokens.
Email Settings	Select to provide the SMTP server name or IP address.
Test Action	<p>Allows you to test the e-mail action.</p>  NOTE: After sending the test e-mail, verify that the e-mail was received successfully and has the expected content.

 **NOTE: Alert tokens are substituted at the time the alert action occurs. They are not substituted for a test action.**

 **NOTE: Certain paging vendors support alphanumeric paging through e-mail. OpenManage Essentials supports paging through the e-mail option.**

Trap Forwarding

Simple Network Management Protocol (SNMP) traps are generated in response to changes in the status of sensors and other monitored parameters on a managed device. To correctly forward these traps, you must configure an SNMP trap destination, defined either by IP address or host name. For information about forwarding SNMPv1 and SNMP v2 traps in both the original format and OMEssentials format, see [Forwarding Alerts Use Case Scenarios](#).

For example, you may want to use trap forwarding if you are in a multi-tiered enterprise environment using OpenManage Essentials to create associations and forward traps to the enterprise manager.

If the trap is being processed locally and then forwarded to the destination or it is just forwarded to the destination.

Use this window to specify the parameters for configuring trap forwarding.

Table 201. Trap Forwarding

Field	Description
Destination	Provide the IP address or host name for the system that is hosting the enterprise management application.
Community	Provide the SNMP community to which the destination IP address or host name belongs.
Forward Trap in Original Format	Select this check box to forward the trap in the same format received by OpenManage Essentials.

Field	Description
Test Action	Forwards a test trap to the specified destination using the specified community string.

SNMP V3 Configuration

The following table describes the fields displayed in the **SNMP V3 Configuration**.

Table 202. SNMP V3 Configuration

Field	Description
Agent IP Address	Provide the SNMP agent IP address.
Engine ID	Provide the unique engine ID of the SNMP agent.
Username	Provide the user name required to execute the task on the device.
Authentication Protocol	Select the authentication protocol for the discovery of the devices. The available options are MD5, SHA1, and none. The device must be configured using the same authentication protocol for the discovery to be successful. If the authentication protocol is selected to be none, then the encryption option is also disabled.
Authentication Password	Provide the authentication password.
Encryption Protocol	Select the encryption protocol for the discovery of the devices. The available options are AES, DES, and none. The device must be configured using the same encryption protocol for the discovery to be successful.
Encryption Password	Provide the encryption password.
Refresh	Click to refresh the SNMP V3 Configuration page to display the added SNMP V3 traps.
Add New	Click to configure the SNMP V3 traps manually.
Import	Click to import the .csv file containing the SNMP V3 trap credentials.
Export	Click to export the SNMP V3 trap credentials to a .csv file.
Save	Click to save the SNMP V3 traps after importing the credentials from a .csv file or by providing the credentials manually.
Delete	Click to delete the selected SNMP V3 traps from the list.

SNMP V3 Configuration Wizard

Table 203. SNMP V3 Configuration Wizard

Field	Description
Agent IP Address	Provide the SNMP agent IP address.
Engine ID	Provide the unique engine ID of the SNMP agent.
Username	Provide the user name required to execute the task on the device.
Authentication Protocol	Select the authentication protocol for the discovery of the devices. The available options are MD5, SHA1, and none. The device must be configured using the same authentication protocol for the discovery to be successful. If the authentication protocol is selected to be none, then the encryption option is also disabled.

Field	Description
Authentication Password	Provide the authentication password.
Encryption Protocol	Select the encryption protocol for the discovery of the devices. The available options are AES, DES, and none. The device must be configured using the same encryption protocol for the discovery to be successful.
Encryption Password	Provide the encryption password.

Category and Sources Association

OpenManage Essentials has many alert categories and sources that are predefined and prepopulated for management agents. Select any of the predefined alert categories or sources to associate it with the alert action or filter. For more information and the complete list of categories and alert sources, see [Alert Categories](#).

Device Association

You can select predefined groups (device types), custom groups, specific devices, or a device query. Device association currently only covers predefined groups.

For custom groups, create a custom group using the **New Custom Group Wizard**. The custom group shows up in the tree.

To use device query, select a query from the list.

Click **New** to create a new device query to search and assign the devices to the alert action.

Click **Edit** to change the query logic.

Select groups or devices from the tree, you can use the query option to create a specific criteria for the selection.

Device Query Options


Table 204. Device Query Options

Field	Description
Select a query	Select a query from the drop-down list.
New	Add a new query.
Edit	Edit an existing query.
All Devices	Select to include all the Devices that is managed in OpenManage Essentials.
Clients	Select to include client devices, such as desktops, portables, and workstations.
HA Clusters	Select to include High Availability server clusters.
KVM	Select to include keyboard video mouse devices.
Microsoft Virtualization Servers	Select to include Microsoft Virtualization Servers.
Modular Systems	Select to include Modular Systems.
Network Devices	Select to include Network Devices.
OOB Unclassified Devices	Select to include out of band Unclassified Devices like Lifecycle Controller enabled devices.
Power Devices	Select to include PDUs and UPS.
Printers	Select to include Printers.
RAC	Select to include devices with Remote Access controllers.

Field	Description
Servers	Select to include Dell servers.
Storage Devices	Select to include storage devices.
Unknown	Select to include unknown devices.
VMware ESX Servers	Select to include VMware ESX servers.
VxFlex Ready Nodes	Select to include VxFlex Ready Nodes and ScaleIO Ready Nodes.

Date and Time Range

Table 205. Date and Time Range

Field	Description
Limit Date Range	Specifies a specific date range to match alerts.
Limit Time Range	Specifies a specific time range to match alerts.
Limit Days	<p>Select to specify the days on which to enable the alert association. If you do not enable this option, the association is applied continuously within the time frame that you specify.</p> <p>Each of these fields are exclusive of the other, so selecting date 8/1/11- 10/1/11, 1am to 4 AM, Friday, will match alerts on only Fridays from 1-4 AM only within that date range.</p> <p> NOTE: It is possible to input a date range and days selection that will never produce a result. For example, 9/1/11 and Monday — since 9/1/11 was a Thursday, it will never match.</p> <p>If none of these are checked, it means that the alert selection will have no date/time filter.</p>

Alert Action — Duplicate Alert Correlation

Table 206. Duplicate Alert Correlation

Field	Description
Yes. Only duplicate alerts that match this filter will be executed.	Enabling this option deletes duplicate alerts (with the same ID and from the same device) received within the specified interval. Use this option to prevent a device from sending an overabundance of alerts to the console.
Ignore duplicate alerts that are received during the interval (1 second - 24 hours).	Select this option and set the required time interval to ignore duplicate alerts. This option can be used to ignore alerts for maximum of 24 hours.
No	Select this option if you do not want duplicate alerts to run at increased duration.

Summary — Alert Action Details

View and edit selections.

The alert action details screen is shown on the final page of the alert action wizards or when clicking any alert action in the tree.

The alert action will have a subset of the following properties, depending on alert action type and filter criteria chosen (this probably should be a table):

Table 207. Summary — Alert Action Details

Field	Description
Name	The name of the alert action.
Action Enabled	Specifies if the alert action is enabled or disabled.
Type	The alert action type — App Launch, Email, Ignore, and Trap Forward.
Description	The description of the alert action.
To	The e-mail addresses to which the e-mail is sent.
From	The e-mail address from whom the e-mail originates.
Subject	The subject of the e-mail which may include alert tokens.
Message	The message of the e-mail which may include alert tokens.
Destination	The destination name or IP address used for trap forwarding.
Community	The community string used for trap forwarding.
Executable Name	The name of the executable, script, or batch file to be used by the alert action.
Arguments	The command line arguments used when invoking the alert action.
Associated Severity	The alert severity criteria used when matching alerts.
Associated Alert Categories	The alert category criteria used when matching alerts.
Associated Alert Sources	The alert source criteria used when matching alerts.
Associated Device Groups	The alert source device group criteria used when matching alerts.
Associated Devices	The alert source device criteria used when matching alerts.
Associated Date Range	The alert date range criteria used when matching alerts.
Associated Time Range	The alert time range criteria used when matching alerts.
Associated Days	The alert days criteria used when matching alerts.
Minimum Repeat Time	If enabled, specifies the minimum time in seconds between two of the same alerts from the same device.

Alert Categories

OpenManage Essentials has many alert categories and sources that are predefined and pre populated for management agents.

Alert categories are organizational levels of the **Alert Categories** tree. Alert sources specify the low level details of each alert. To monitor the alert categories and sources, apply an alert action association to the alert source or to its parent category.

This page provides a list of categories and the alerts sources within that category. Use this page to configure alerts based on categories.

Alert Categories Options

Table 208. Alert Categories Options

Field	Description
Brocade-Switch	Select this category to include alerts for Brocade-Switch.
Compellent	Select this category to include alerts for Compellent storage devices.

Field	Description
Advanced Infrastructure Management	Select this category to include alerts for Advanced Infrastructure Management.
Environmental	Select this category to include alerts for temperature, fan enclosure, fan speed, thermal, and cooling.
EqualLogic Storage	Select this category to include alerts for EqualLogic storage.
FC-Switch	Select this category to include alerts for Fibre Channel switches.
General Redundancy	Select this category to include alerts for General Redundancy.
HyperV Server	Select this category to include alerts for HyperV Server.
iDRAC	Select this category to include alerts for iDRAC.
Juniper-Switch	Select this category to include alerts for Juniper switches.
Keyboard-Video-Mouse (KVM)	Select this category to include alerts for KVMs.
Memory	Select this category to include alerts for memory.
Network	Select this category to include alerts related to Dell Networking switches.
Other	Select this category to include alerts for other devices.
PDU	Select this category to include alerts for PDUs.
Physical Disk	Select this category to include alerts for physical disks.
Power	Select this category to include alerts for power.
Power Center	Select this category to include alerts for power center.
Printers	Select this category to include alerts for printers.
Processor	Select this category to include alerts for processor.
Removable Flash Media	Select this category to include alerts for removable flash media.
Security	Select this category to include alerts for security.
Storage Enclosure	Select this category to include alerts for storage enclosures.
Storage Peripheral	Select this category to include alerts for storage peripherals.
Storage Software	Select this category to include alerts for storage software.
System Events	Select this category to include alerts for system events.
Tape	Select this category to include alerts for tape drives.
Test Events	Select this category to include alerts for test events.
Unknown	Select this category to include unknown alerts related statuses.
UPS	Select this category to include alerts for UPS.
Virtual Disk	Select this category to include alerts for virtual disks.
VMware ESX Server	Select this category to include alerts for VMware ESX servers.

Edit Trap Definitions

Table 209. Edit Trap Definitions

Field	Description
Trap Name or Enterprise OID	Field to provide the trap name or enterprise OID of the trap you want to edit.
Search	Click to search the OpenManage Essentials database for the trap name or enterprise OID that you provided.
Event Category	Click to display the event categories defined in the OpenManage Essentials database. You can select a category to display all the traps defined for that category in the Edit Trap(s) grid. You can also navigate and select a particular trap from the category.
Edit Traps	
Name	Displays the trap name.
Category Name	Displays the category name of the trap.
Severity	Displays the severity of the trap.
Format String	Displays the message string that is displayed in the OpenManage Essentials alert logs.
Enterprise OID	Displays the enterprise OID (SNMP OID prefix) of the event source that you want to monitor.
Description	Displays the trap description.
Generic Trap ID	Displays the generic trap ID of the SNMP trap that you want to monitor from the required event source.
Specific Trap ID	Displays the specific trap ID of the SNMP trap that you want to monitor from the required event source.
Save	Click to save the changes to the OpenManage Essentials database.

Alert Source

Each Alert Category contains alert sources. Click an alert category to view alert sources. Expand a category to view the list of alert sources, and select an alert source.

Table 210. Alert Source

Field	Description
Name	The name of the new alert source, for example, myFanAlert.
Type	The protocol information.
Catalog	Provides the catalog information.
Severity	Specifies the severity assigned to the alert that is triggered if the alert source generates the specified SNMP trap.
Format string	Provides the message string that appears in the Alert Logs if the alert source generates an alert of sufficient severity to trigger the alert. You can use formatting commands to specify parts of

Field	Description
	the message string. For SNMP, the valid formatting commands are: \$N = system name \$d = date \$t = time \$s = severity \$e = enterprise object identifier (OID) \$sp = specific trap OID \$g = generic trap OID \$1 - \$# = varbind values
SNMP Enterprise OID	Provides the enterprise OID (SNMP OID prefix) of the management information base (MIB) file that defines the event source that you want to monitor.
SNMP Generic Trap OID	Provides the generic trap ID of the SNMP trap that you want to monitor from the desired event source. See the <i>Dell OpenManage Server Administrator SNMP Reference Guide</i> at Dell.com/OpenManageManuals for more information on SNMP traps.
SNMP Specific Trap OID	Provides the specific trap ID of the SNMP trap that you want to monitor from the desired event source. See the <i>Dell OpenManage Server Administrator SNMP Reference Guide</i> at Dell.com/OpenManageManuals for more information on SNMP traps.

Manage MIBs

Manage MIBs Pane

The Manage MIBs pane consists of:

- **Import MIB** view — To import the MIB file. See [Importing the MIB File](#).
- **Remove MIB** view — To remove the MIB file from the OpenManage Essentials database. See [Removing the MIB File from OpenManage Essentials](#).

Manage Traps Pane



The Manage Traps pane consists of:

- **Custom Trap Definitions** view — To add trap definitions to OpenManage Essentials database. See [Adding Traps](#).
- **Reset Built-in Trap Definitions** view — To reset a pre-defined trap that you edited. See [Reverting Traps](#).

Import MIB

Table 211. Import MIB

Field	Description
Select files for upload	Displays the MIB files that you have selected for upload.
Select the MIB File	Displays the path of the file selected for parsing.
Browse	Click to navigate to the file location.
Event Details	

Field	Description
Category Name	Select to display the event category names defined in OpenManage Essentials and the category name of the parsed MIB.
Severity	Select to display the severity defined in OpenManage Essentials.
Apply the selected event category to all traps	Select to change the category name of all the traps.  NOTE: If you do not select the check box, you have to manually select the traps and select the category name from the drop-down list.
Apply the selected severity to all traps	Select this check box to change the severity of all the traps.  NOTE: If you do not select the check box, you have to manually select the traps and select the severity from the drop-down list.
Traps Available for Import	
Name	Displays the trap name from the MIB file.
Category Name	Displays the category name of the trap.
Severity	Displays the severity of the trap. You can modify the severity of the trap to: <ul style="list-style-type: none"> • Unknown • Info • Normal • Warning • Critical • By Value. See Severity Configuration By Value.
Format String	Displays the trap description.
Enterprise OID	Displays the enterprise OID (SNMP OID prefix) of the MIB file that defines the event source that you want to monitor.
Description	Displays the description of the trap.
Generic Trap ID	Displays the generic trap ID of the SNMP trap that you want to monitor from the required event source.
Specific Trap ID	Displays the specific trap ID of the SNMP trap that you want to monitor from the required event source.
Reset All	Click to revert the severity of all the traps to the default values.
Import Traps	Click to import traps to the OpenManage Essentials database.

Severity Configuration by Value

The Severity Configuration By Value window enables you to specify the severity of the alert based on the value of one or more variable bindings associated with the trap.

Table 212. Severity Configuration by Value

Field	Description
Trap Variable	Displays the trap variable index.
Severity	Displays the severity assigned for each object value or object ID.
Object ID	Displays the numerical value based on the trap variable index.
Object Value	Displays the string value based on the trap variable index.
Add New	Click to add the severity configuration.
Select the Variable	Select the trap variable that you want to update.
OK	Click to save the changes.
Reset	Click to revert the severity of the trap to the default values.

Remove MIB

Table 213. Remove MIB

Field	Description
Imported MIB(s)	Displays the list of MIBs that are imported in the OpenManage Essentials database.
Remove MIB	Click to remove the imported MIBs from the OpenManage Essentials database.

Troubleshooting MIB Import

Issue: The MIB Import displays the following error message: Dependent MIB files need to be imported. Please import: RFC1155-SMI to the Mib Repository before continuing to import this Mib.

Cause: An MIB file may be dependent on another MIB file. While parsing a source MIB file, all the files referred by the source MIB file must be present in the reference directory or the MIB repository. The error message is displayed because the referred MIB file is missing from the reference directory.

Resolution: To resolve this issue:

- Ensure that you have administrator privileges in OpenManage Essentials. You must launch OpenManage Essentials at least once before importing the MIB file.
- Retrieve the missing MIB file and add the file to the reference directory. If there are multiple dependencies of the parent MIB on more than one file, import all the required MIB files, and then parse the parent MIB file.

 **NOTE:** The above resolution also applies for an invalid MIB file.

Issue: Unable to parse the MIB file.

Resolution: Check the logs to see if there are any MIB compiler issues. If there are no compiler issues, compile the MIB using a standard MIB compiler and verify whether the MIB is properly defined.

Issue: Unable to import the parsed trap definitions into OpenManage Essentials after parsing the MIB file.

Resolution: See the *Readme* at `C:\Program Files (x86)\Dell\MIBImport` for the list of MIB files that cannot be imported into OpenManage Essentials.

Manage Traps

Custom Trap Definitions

Table 214. Custom Trap Definitions

Field	Description
Add Trap	
Category Name	To select the event category names defined in OpenManage Essentials or to provide a new category name.
Unknown Traps	Click to display the unknown traps received in OpenManage Essentials.
Description	To provide the trap description.
Trap Name	To provide or edit the trap name.
Generic ID	To provide or edit the generic trap ID of the SNMP trap that you want to monitor from the required event source.
Enterprise OID	To provide or edit the enterprise OID (SNMP OID prefix) of the event source that you want to monitor.
Specific ID	To provide the specific trap ID of the SNMP trap that you want to monitor from the required event source.
Format String	To provide or edit the message string that is displayed in the OpenManage Essentials alert logs.
Severity	Displays the severity of the trap. You can modify the severity of the trap to: <ul style="list-style-type: none"> • Unknown • Info • Normal • Warning • Critical • By Varbind Value. See Severity Configuration By Value.
Add Trap	Click to add the trap definition to the User-defined Trap(s) grid.
Delete User-Defined Traps	
Name	Displays the trap name.
Category Name	Displays the category name of the trap.
Severity	Displays the severity of the trap.
Enterprise OID	Displays the enterprise OID (SNMP OID prefix) of the event source that you want to monitor.
Description	Displays the trap description
Format String	Displays the message string that is displayed in the OpenManage Essentials alert logs.

Field	Description
Generic Trap ID	Displays the generic trap ID of the SNMP trap that you want to monitor from the required event source.
Specific Trap ID	Displays the specific trap ID of the SNMP trap that you want to monitor from the required event source.
Delete Trap	Click to delete the selected traps.



Reset Built-in Trap Definitions

Table 215. Reset Built-in Trap Definitions




Field	Description
Edited Traps	
Name	Displays the trap name.
Category Name	Displays the category name of the trap.
Severity	Displays the severity of the trap.
Enterprise OID	Displays the enterprise OID (SNMP OID prefix) of the event source that you want to monitor.
Format String	Displays the message string that is displayed in the OpenManage Essentials alert logs.
Description	Displays the trap description
Generic Trap ID	Displays the generic trap ID of the SNMP trap that you want to monitor from the required event source.
Specific Trap ID	Displays the specific trap ID of the SNMP trap that you want to monitor from the required event source.
Revert Traps	Click to revert the state of the selected traps to the original state in the OpenManage Essentials database.

Updating BIOS, firmware, drivers, and system applications

With the System Update feature in OpenManage Essentials, you can:

- Upgrade and downgrade firmware, drivers, BIOS, application, and OpenManage Server Administrator.
 - Compare the drivers and firmware on the inventoried servers and modular blade enclosures with a source catalog and update them if needed.
-  **NOTE:** The recommended minimum network bandwidth that is required for OpenManage Essentials in a WAN environment is 10 Mbps (for monitoring) and 20 Mbps (for updates). Inventory automatically starts after the updates are applied to a target server.
-  **NOTE:** OpenManage Essentials supports system updates on PowerEdge 11th, 12th, 13th, and 14th generation servers using iDRAC with Lifecycle Controller.
- Filter devices by clicking the **Filtered by** option. You can either select a query or select the devices/groups from the device tree.

Check for these prerequisites before you update systems:

- Internet is accessible, and you can access **downloads.dell.com** (port 443)—if you are using the online catalog source.
 - DNS is resolved.
-  **NOTE:** When providing system credentials, if the username has spaces or periods, the username must be provided within quotation marks. For example, "localhost\johnny marr" or "us-domain\tim verlaine". Spaces and periods can be used in usernames for OpenManage System Administrator Tasks, Generic Command Line Tasks (local system), OpenManage Systems Administrator Deployment Tasks. System Updates (In Band, through OpenManage System Administrator) also support spaces and periods. Out of Band updates (through RAC device) or commands such as RACADM do not support space or period in the username.
-  **NOTE:** If a deployment task is run on a target server that is configured with a BIOS System Password, when the task is running, ensure that you launch the iDRAC virtual console, and if prompted, enter the system password. Else, the task might display running state for some time and eventually timeout.
-  **NOTE:** If there are both 32-bit and 64-bit versions of OpenSSL libraries that are installed on an RHEL system, Dell EMC recommends to uninstall the 32-bit version. Also, if there is a symbolic link to `libcrypto.so.6` created by OpenManage Essentials, remove the symbolic link, and then redeploy BIOS, firmware, drivers, and system applications.

Viewing the System Update page

To view the System Update page, click **Manage** → **System Update**.

By default, the System Update page displays all the discovered devices. You can use the **Filtered by:** link to display only the selected devices or device groups.

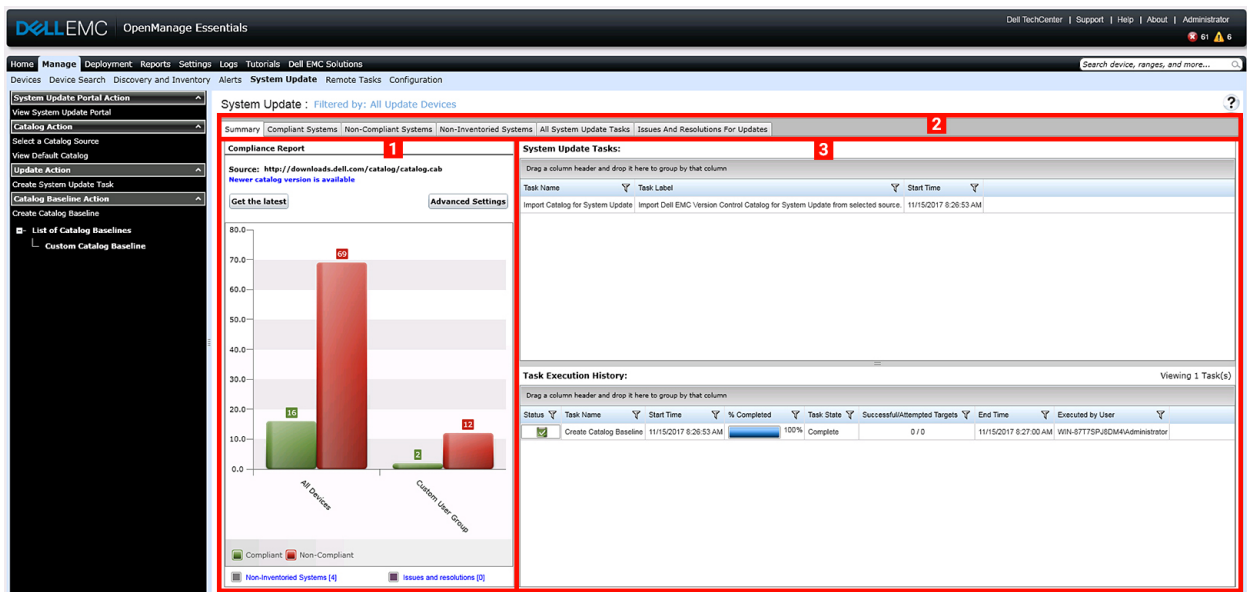


Figure 34. System Update page

1. Compliance report. See [Compliance Report](#)
2. Tabbed systems information. See [Compliant Systems](#), [Non Compliant Systems](#), [Non Inventoried Systems](#), and [Issues and Resolutions](#).
3. System update tasks. See [All System Update Tasks](#)

Understanding sources of system updates

- **Online source**—Default option which downloads latest driver and firmware versions from **downloads.dell.com**. This is also a default option for updating MX Chassis devices.
- **NOTE:** OpenManage Essentials automatically checks for system updates and displays a message if a newer version is available.
- **File system source**—Drivers and firmware from the OpenManage Server Update Utility (SUU) media.
- **Repository Manager file**—Customized selection of specific drivers and firmware generated from the Repository Manager tool.

Choosing the right source of system updates

- **Recommended option**—Use the online source to ensure that you consistently have the latest drivers and firmware available from Dell EMC or use the Server Update Utility (SUU) option for a qualified set of drivers and firmware.
- **Create custom catalog**—Using this option gives you maximum control over driver and firmware revisions in your environment because you select them individually from either the SUU media or online source using the Repository Manager. You can install Repository Manager, a separate tool, from the OpenManage Essentials installation package.

Selecting an update catalog source

1. Click **Manage** → **System Update** → **Select a Catalog Source**.
2. In **Select a Catalog Source**:
 - Select one of the update sources.
 - For MX7000 chassis, select the **Use an online source** option, and then select the preferred protocol.
3. Click **Import now**.

Viewing comparison results

This section provides information required to view the results of the comparison of devices to a source catalog.



Viewing compliant systems

1. Click **Manage** → **System Update**.
2. To view the compliant systems, click **Compliant Systems**.
For a MX7000 chassis, compliance details of the lead chassis, member chassis, and compute sleds are listed individually.

Viewing noncompliant systems

1. Click **Manage** → **System Update**.
2. To view the noncompliant systems, click **Non-Compliant Systems**.
Devices with the driver and firmware versions that are different from the catalog are displayed. For a MX7000 chassis, noncompliance details of the lead chassis, member chassis, and compute sleds are listed individually.

Viewing non-inventoried systems

1. Click **Manage** → **System Update**.
2. To view the non-inventoried systems, click **Non-Inventoried Systems**.
 **NOTE: CMC firmware updates (CMC active controller only) are also displayed in these results.**
 **NOTE: To inventory the non-inventoried servers, you can select the non-inventoried servers and click Inventory. The method of inventory collection may vary based on the following criteria:**
 - If the server is discovered through SNMP and has OMSA installed, the default discovery and inventory is initiated.
 - If the server is discovered through WMI/SSH and does not have OMSA installed, the **Create F/W & Driver Inventory Task** window is displayed.

Viewing systems with issues and resolutions

1. Click **Manage** → **System Update**.
2. Click the **Issues and Resolutions For Updates** tab.
For more information about the update issues and the possible resolutions, see [Issues and Resolutions Use Case Scenarios](#).

Creating a catalog baseline

1. Click **System Update** → **Create Catalog Baseline**.
The Create Catalog Baseline wizard with a baseline name is displayed.
2. Enter to change the baseline name.
3. Click **Browse** to navigate to the file system and select the repository manager file.
4. Click **Import Now**.
The catalog is listed under **List of Catalog Baselines**, and the baseline details are displayed on the **Baseline details** page.

Viewing the Default Catalog

Select to view the catalog file that is currently in use for applying software updates.

Table 216. View Default Catalog

Field	Description
Source	Displays the source. The source is either Server Update Utility, downloads.dell.com, or Repository Manager.
Source Type	The type for source from which the catalog file is taken. For example, downloads.dell.com.
Release ID	The unique identification number assigned to the released catalog file.
Release Date	The date on which the catalog file was released.
Newer version available	Displays if a newer version is available.

System Update Use Case Scenarios

The following table provides use case scenarios about how system updates occur based on different protocols and the update modes.





 **NOTE:** If the preferred system update method selected in Advanced Settings is In-Band (Operating System) and OpenManage Server Administrator (OMSA) is installed on the target server, the components are updated using OMSA. If OMSA is not installed on the target server, the components are updated through the operating system.

Table 217. System Update Use Case Scenarios

Protocol Used for Server IP Discovery and Inventory	Protocol Used for iDRAC IP Discovery and Inventory	Preferred System Update Mode Selected in Advanced Settings	Credentials for System Update	Actual Update Mode
SNMP	SNMP	In-Band (Operating System)	Server	All components are updated using OpenManage Server Administrator.
SNMP	SNMP	Out-of-Band (iDRAC)	Server	 NOTE: When an iDRAC IP is discovered using SNMP, iDRAC software inventory is not retrieved and all components are updated are using Server Administrator irrespective of the preferred system update mode selected.
WMI	SNMP	In-Band (Operating System)	Server	All components are updated using OpenManage Server Administrator.
WMI	SNMP	Out-of-Band (iDRAC)	Server	All components are updated using Server Administrator because the protocol used for iDRAC discovery and inventory was SNMP.
WMI	SNMP	In-Band (Operating System)	Server	All components are updated using the operating system.
SSH	WS-Man/SNMP	In-Band (Operating System)	Server	All components are updated using the operating system.
SNMP	WS-Man	In-Band (Operating System)	Server	All components are updated using OpenManage Server Administrator.

Protocol Used for Server IP Discovery and Inventory	Protocol Used for iDRAC IP Discovery and Inventory	Preferred System Update Mode Selected in Advanced Settings	Credentials for System Update	Actual Update Mode
SNMP	WS-Man	Out-of-Band (iDRAC)	iDRAC	<p>BIOS, firmware, and applications are updated using iDRAC.</p> <p> NOTE: When an iDRAC IP is discovered using WS-Man, the iDRAC software inventory is retrieved and the components are updated using iDRAC.</p> <p>However, if drivers are present in addition to BIOS, firmware, and applications, then all the components are updated using Server Administrator and not iDRAC.</p>
WMI	WS-Man	In-Band (Operating System)	Server	All components are updated using OpenManage Server Administrator.
WMI	WS-Man	Out-of-Band (iDRAC)	iDRAC	<p>BIOS, firmware, and applications are updated using iDRAC.</p> <p> NOTE: When an iDRAC IP is discovered using WS-Man, the iDRAC software inventory is retrieved and the components are updated using iDRAC.</p> <p>However, if drivers are present in addition to BIOS, firmware, and applications, then all the components are updated using Server Administrator and not iDRAC.</p>
WS-Man (ESXi-based server)	WS-Man (ESXi-based server)	In-Band (Operating System)	iDRAC	All components are updated using iDRAC. For ESXi-based servers, all components are updated using iDRAC , irrespective of preferred system update mode selected.
WS-Man (ESXi-based server)	WS-Man (ESXi-based server)	Out-of-Band (iDRAC)	iDRAC	
Not applicable. The server IP is not discovered.	WS-MAN	In-Band (Operating System)	iDRAC	All components are updated using iDRAC.
Not applicable. The server IP is not discovered.	WS-MAN	Out-of-Band (iDRAC)	iDRAC	

Applying system updates by using the Non-Compliant Systems tab

 **NOTE: The following are some of the considerations when applying system updates:**

- You can only update systems using iDRAC6 or later if they are discovered using the WS-Man protocol.
- If the iDRAC firmware version is 1.40.40 or earlier, applying system updates out-of-band (iDRAC) is supported only for 32-bit Dell Update Packages (DUPs). If you select a catalog that has no 32-bit DUPs for applying an out-of-band system update, OpenManage Essentials does not display any updates under **Select Updates to Apply**.
- Applying system updates in-band (Operating System) requires that the **Windows Management Instrumentation** service is running on the selected targets.
- Applying system updates requires the availability of the default **Temp** folders (C:\Windows\Temp and C:\Users\<username>\AppData\Local\Temp). Ensure that the **Temp** folders are not deleted or moved.
- For out-of-band system updates, Dell recommends that system on which OpenManage Essentials is installed and the iDRAC should be on the same network. If they are on different network, the system update task cannot be performed successfully. If you are using Active Directory authentication for the iDRAC, it is recommended that system on which OpenManage Essentials is installed and the iDRAC should be on the same network domain.
- In an MCM group, system updates can be applied only to the lead MX7000 chassis.

To apply system updates:

1. Click **Manage** → **System Update**.
2. Click the **Non-Compliant Systems** tab.

 **NOTE: You can also filter systems based on either the groups or the devices by clicking the Filtered by: link. Select the devices in the Select System Update Target Devices and Device Groups window and click Apply.**

3. Select the systems from the list that you want to update.

 **NOTE: You can update multiple systems at the same time.**

 **NOTE: The following are the considerations when using 64-bit DUPs for system update:**

- For in-band updates (Operating System) – If the selected target is a server running a Windows 64-bit operating system, all applicable 64-bit packages are available for update. If the catalog does not contain 64-bit packages for a component, the corresponding 32-bit package is available for update.
- For out-of-band updates (iDRAC) – If the selected target is an iDRAC of a 12th or 13th generation PowerEdge server and has iDRAC firmware version later than 1.40.40 installed, all applicable 64-bit packages are available for update. If the catalog does not contain 64-bit packages for a component, the corresponding 32-bit package is available for update.
- For in-band or out-of-band updates – If the selected 12th or 13th generation PowerEdge server is running a 32-bit operating system and has iDRAC firmware version later than 1.40.40 installed, by default, only 32-bit packages are available for update unless there is a package that is known only to iDRAC and not known to OMSA.

4. Click **Apply Selected Updates**.

A window is displayed to schedule updates.

 **NOTE: Chassis and blades are not associated for updates. They are treated as individual components and you must manually select them.**

 **NOTE: Chassis, blade server BIOS, and iDRAC version interdependency management is not available.**

5. Enter a task name.
6. Review the selected updates.
7. Set the task schedule to **Run Now**, or set a specific date and time.
8. If you want to apply the changes immediately, select **After update, if required, reboot the target server**.


The **Out-of-band Reboot Type** option is displayed.

Using the **Out-of-band Reboot Type** option, you can set the types of reboot methods available for the system update. The reboot methods are:

- **Power Cycle (Cold)**—Select this option to power off and then restart the system.
- **Graceful Reboot without forced shutdown (Warm)**—Select this option to shut down and then reboot the operating system without forcefully turning off the target system.
- **Graceful Reboot with forced shutdown (Warm with forced)**—Select this option to shut down and then reboot the operating system by forcefully turning off the target system.

 **NOTE: By default, the Graceful Reboot with forced shutdown reboot method is selected.**

9. If you want to skip the signature and hash check on the system update package, select **Skip Signature and Hash Check**.
10. For out-of-band update only—If you experience failures while performing updates using the iDRAC, select **Before update, reset the iDRAC**.

 **CAUTION: If the Before update, reset the iDRAC option is selected, all iDRAC jobs that are currently in the queue are deleted before the update is applied. If required, you must create the jobs again.**

11. Enter the administrator credentials of the operating system or iDRAC for the target device.

 **NOTE: For applying system updates on target systems running a Windows operating system with the User Account Control (UAC) feature enabled:**

- If the target system is part of a Domain, you must provide the credentials of either the Domain Administrator or a member in the Administrators group. Do not provide the credentials of the local, non-domain account on the target system, even if the account is in the Administrators group.
- If the target system is not part of a Domain, you must provide the Administrator credentials. If you want to provide the credentials of a non-default Administrator account, ensure that the Remote WMI permissions are enabled for that user account.

Examples: In a Windows domain environment, enter <Domain\Administrator> and password. In a Windows workgroup environment, enter <LocalHost\Administrator> and the password.

In a Linux environment, enter root and password. If you want to apply system updates using sudo, select **Enable Sudo** and update the **SSH port number**.

 **NOTE: Before you apply system updates using sudo, create a user account, edit the sudoers file using the visudo command, and add the following:**

For target systems running a 32-bit operating systems:

```
Cmnd_Alias OMEUPDATE = /bin/tar,/opt/dell/srvadmin/bin/omexec,/tmp/  
LinuxPreInstallPackage/runbada,/tmp/LinuxPreInstallPackage/omexec,/tmp/invcol.bin  
<sudo_username> ALL=OMEUPDATE,NOPASSWD:OMEUPDATE
```

For target systems running a 64-bit operating systems:

```
Cmnd_Alias OMEUPDATE = /bin/tar,/opt/dell/srvadmin/bin/omexec,/tmp/  
LinuxPreInstallPackage64/runbada,/tmp/LinuxPreInstallPackage64/omexec,/tmp/  
invcol64.bin <sudo_username> ALL=OMEUPDATE,NOPASSWD:OMEUPDATE
```

 **NOTE: Applying system updates using sudo is not supported for SUSE Linux Enterprise Server targets.**

12. Click **Finish**.

 **NOTE: You cannot schedule Windows and Linux updates to occur using the same task, and separate tasks should be created.**

Applying System Updates by using the System Update Task wizard

The system update task allows you to view and select non-compliant systems and their applicable updates.



NOTE: The following are some of the considerations when applying system updates:

- You can only update systems using iDRAC6 or later if they are discovered using the WS-Man protocol.
- If the iDRAC firmware version is 1.40.40 or earlier, applying system updates out-of-band (iDRAC) is supported only for 32-bit Dell Update Packages (DUPs). If you select a catalog that has no 32-bit DUPs for applying an out-of-band system update, OpenManage Essentials does not display any updates under **Select Updates to Apply**.
- Applying system updates in-band (Operating System) requires that the **Windows Management Instrumentation** service is running on the selected targets.
- Applying system updates requires the availability of the default **Temp** folders (C:\Windows\Temp and C:\Users\<username>\AppData\Local\Temp). Ensure that the **Temp** folders are not deleted or moved.
- For out-of-band system updates, Dell recommends that system on which OpenManage Essentials is installed and the iDRAC should be on the same network. If they are on different network, the system update task cannot be performed successfully. If you are using Active Directory authentication for the iDRAC, it is recommended that system on which OpenManage Essentials is installed and the iDRAC should be on the same network domain.
- In an MCM group, system updates can be applied only to the lead MX7000 chassis.

To create a system update task:

1. Click **Manage** → **System Update**.
The **System Update** portal is displayed.
2. In the **Update Action** section, click **Create System Update Task**.
The **Non-Compliant Systems** page of **System Update** wizard is displayed.
3. Select any noncompliant systems that you want to update and click **Next**.



NOTE: You can update multiple systems at the same time.



NOTE: The following are the considerations when using 64-bit DUPs for system update:

- For in-band updates (Operating System) – If the selected target is a server running a Windows 64-bit operating system, all applicable 64-bit packages are available for update. If the catalog does not contain 64-bit packages for a component, the corresponding 32-bit package is available for update.
- For out-of-band updates (iDRAC) – If the selected target is an iDRAC of a 12th or 13th generation Dell PowerEdge server and has iDRAC firmware version later than 1.40.40 installed, all applicable 64-bit packages are available for update. If the catalog does not contain 64-bit packages for a component, the corresponding 32-bit package is available for update.
- For in-band or out-of-band updates – If the selected 12th or 13th generation PowerEdge server is running a 32-bit operating system and has iDRAC firmware version later than 1.40.40 installed, by default, only 32-bit packages are available for update unless there is a package known only to iDRAC and not known to OMSA.

The **Applicable Packages** page is displayed.

4. Select the packages that you want to update and click **Next**.
The **Summary and Credentials** page is displayed.
5. Type a name for the task in the appropriate field.
6. In the **Set the Task Schedule** section:
 - a. Set the task schedule to **Run Now** or set a specific date and time.
 - b. If you want to apply the changes immediately, select **After update, if required, reboot the target server**.

The **Out-of-band Reboot Type** option is displayed.

Using the **Out-of-band Reboot Type** option, you can set the types of reboot methods available for the system update. The reboot methods are:

- **Power Cycle (Cold)** — Select this option to power off and then restart the system.
- **Graceful Reboot without forced shutdown (Warm)** — Select this option to shut down and then reboot the operating system without forcefully turning off the target system.

- **Graceful Reboot with forced shutdown** (Warm with forced) — Select this option to shut down and then reboot the operating system by forcefully turning off the target system.

 **NOTE: By default, the Graceful Reboot with forced shutdown reboot method is selected.**

- If you want to skip the signature and hash check on the system update package, select **Skip Signature and Hash Check**.
- For out-of-band update only — If you experience failures while performing updates using the iDRAC, select **Before update, reset the iDRAC**.

 **CAUTION: If the Before update, reset the iDRAC option is selected, all pending jobs or activities scheduled on the iDRAC will be cancelled before the update is applied. If required, you must create the iDRAC jobs again.**


- In the **Enter Credentials for the task execution** section, type the user name and password of the iDRAC (for out-of-band updates) or operating system (for in-band updates).

 **NOTE: For applying system updates on target systems running a Windows operating system with the User Account Control (UAC) feature enabled:**

- If the target system is part of a Domain, you must provide the credentials of either the Domain Administrator or a member in the Administrators group. Do not provide the credentials of the local, non-domain account on the target system, even if the account is in the Administrators group.
- If the target system is not part of a Domain, you must provide the Administrator credentials. If you want to provide the credentials of a non-default Administrator account, ensure that the Remote WMI permissions are enabled for that user account.

Examples: In a Windows domain environment, enter <Domain\Administrator> and password. In a Windows workgroup environment, enter <LocalHost\Administrator> and the password

In a Linux environment, enter root and password. If you want to apply system updates using sudo, select **Enable Sudo** and update the **SSH port number**.

 **NOTE: Before you apply system updates using sudo, create a new user account, edit the sudoers file using the visudo command, and add the following:**

For target systems running a 32-bit operating systems:

```
Cmnd_Alias OMEUPDATE = /bin/tar,/opt/dell/srvadmin/bin/omexec,/tmp/
LinuxPreInstallPackage/runbada,/tmp/LinuxPreInstallPackage/omexec,/tmp/invcol.bin
<sudo_username> ALL=OMEUPDATE,NOPASSWD:OMEUPDATE
```

For target systems running a 64-bit operating systems:

```
Cmnd_Alias OMEUPDATE = /bin/tar,/opt/dell/srvadmin/bin/omexec,/tmp/
LinuxPreInstallPackage64/runbada,/tmp/LinuxPreInstallPackage64/omexec,/tmp/
invcol64.bin <sudo_username> ALL=OMEUPDATE,NOPASSWD:OMEUPDATE
```

 **NOTE: Applying system updates using sudo is not supported for SUSE Linux Enterprise Server targets.**

- Click **Finish**.

 **NOTE: You cannot schedule Windows and Linux updates to occur using the same task, and separate tasks should be created.**

Viewing status of the System Update task

To view and confirm that updates were applied successfully, click **Manage** → **System Update** → **Summary**. The **Task Execution History** pane displays if the updates were applied successfully.

Updating systems without OpenManage Server Administrator

To update the firmware, BIOS, and drivers on a system that does not have OpenManage Server Administrator (OMSA) installed:

1. Collect the software inventory from the server. See [Collecting Firmware and Driver Inventory](#).
2. Update the system through the system update portal. See [Applying System Updates Using the Non-Compliant Systems Tab](#) or [Applying System Updates Using the System Update Task Wizard](#).

Issues and Resolutions Use Case Scenarios

The following table provides information about the issues that are displayed in the **Issues and Resolutions for Updates** tab with the possible resolutions.

Table 218. Issues and Resolutions Use Case Scenarios

Issue	Resolution
PowerEdge VRTX was inventoried using either SNMP or IPMI.	Perform discovery and inventory of PowerEdge VRTX using WS-Man.
iDRAC was inventoried using either SNMP or IPMI.	Perform discovery and inventory of iDRAC using WS-Man.
iDRAC does not meet the minimum version requirements.	Minimum supported iDRAC version for modular servers is 2.20 and for monolithic servers is 1.4. Manually install the required iDRAC versions to proceed.
iDRAC does not have the required license.	iDRAC requires license to perform system updates which can be obtained using License Manager.
The server does not have Server Administrator installed on it or is discovered using SSH. This issue occurs if: <ul style="list-style-type: none">• A Windows-based server without Server Administrator is discovered using WMI.• A Linux-based server with or without Server Administrator is discovered using SSH.	Schedule Inventory Collection Task. Recommended to schedule Periodic Inventory Collection Task.

Configuring automatic purging of downloaded system update files

To apply system updates and to perform remote tasks on target devices, OpenManage Essentials might download the appropriate BIOS, firmware, driver, and application files. By default, the downloaded files are saved in the **<install location>\Essentials\System Update** folder. You can configure OpenManage Essentials to automatically purge some of the downloaded files if the downloads folder (**<install location>\Essentials\System Update**) reaches a defined size limit.


 **NOTE: By default, the purging of downloaded files is disabled.**

To configure automatic purging of downloaded files:

1. Click **Settings** → **Purge Download Settings**.
The **Purge Download Settings** page is displayed.
2. Select **Enable purging of downloaded files** to allow the automatic purging of the downloaded files using the default settings.
3. If required, set the size limit of the downloads folder based on your preference.

 **NOTE: Purging of the downloaded files is initiated when the downloads folder reaches the defined size limit.**

4. If required, set the approximate size of the downloaded files to be purged based on your preference.

 **NOTE: Files in the downloads folder are purged until the total size of the purged files reaches or exceeds the approximate size that you have defined.**

5. Click **Apply**.

System Update — Reference

You can access the following:

- System Update Portal Action
 - View System Update Portal
 - Summary
 - Compliance Report
 - System Update Tasks
 - Tasks Execution History
 - Compliant Systems
 - Non Compliant Systems
 - Non-Inventoried Systems
 - All System Update Tasks
 - Issues and resolutions for updates
- Catalog Action
 - Select a Catalog Source
 - View Default Catalog
 - View MX Chassis Default Catalog
- Update Action
 - Create System Update Task
- Catalog Baseline Action
 - Create Catalog Baseline
 - View Catalog Baseline Associations
 - List of Catalog Baselines

Related links

[Updating BIOS, firmware, drivers, and system applications](#)

[Viewing the System Update page](#)

[Compliance Report](#)

[Non-Compliant Firmware and Drivers](#)

[System Update Task](#)

[Non-Inventoried Systems](#)

[All System Update Tasks](#)

[Issues and Resolutions](#)

Filter Options

Table 219. Filter Options

Filter Option	Description
Is equal to	Select to create the <i>same as</i> logic.
Is not equal to	Select to create the different from logic.
Starts with	Select to filter search based on a text chunk's initial alphanumeric characters. Provide the starting alphanumeric characters in the field.
Ends with	Select to filter search based on a text chunk's final alphanumeric characters. Provide the ending alphanumeric characters in the field.
Contains	Select to filter search based on alphanumeric characters present in a text chunk. Provide the alphanumeric characters in the field.
Does not contain	Select to include the <i>not present</i> logic in search based on alphanumeric characters present in a text chunk.
Is contained in	Select to include the <i>is present</i> logic in an alphanumeric character string.
Is not contained in	Select to include the <i>not present</i> logic in an alphanumeric character string.
Is less than	Select to find a value that <i>is less than</i> the value you provide.
Is less than or equal to	Select to find a value that <i>is less than or equal to</i> the value you provide.
Is greater than	Select to find a value that <i>is greater than</i> the value you provide.
Is greater than or equal to	Select to find a value that <i>is greater than or equal to</i> the value you provide

System Update

This page provides the following information:

- Summary
- Compliant Systems
- Non Compliant Systems
- Non-Inventoried System
- All System Update Tasks
- Issues and Resolutions For Updates

Related links

[Compliance Report](#)
[Non-Compliant Firmware and Drivers](#)
[Non-Inventoried Systems](#)
[All System Update Tasks](#)

Compliance Report



The compliance report provides a bar chart distribution of compliant and noncompliant systems. Click a bar chart portion to view more information on the systems in a pie chart and the software update tasks.



Related link

[System Update](#)

Compliance Report Options

Table 220. Compliance Report Options

Field	Description
Default Catalog Source	Report source
MX Chassis Default Catalog Source	Report source for MX7000 chassis—lead chassis, member chassis, compute sleds, and storage
Get the latest	This option is disabled if the catalog version is the latest. Else, it is active. Click this option to get the latest catalog version.
Advanced Settings	<p>Using these options you can set preferences for upgrading and downgrading firmware, BIOS, driver, and application versions:</p> <ul style="list-style-type: none"> • Enable Downgrades — Select this option to install versions of firmware, BIOS, drivers, and applications that are earlier than the versions installed on the systems. • Disable Downgrades — This option is set by default, selecting this option enables you to install versions of firmware, BIOS, drivers, and applications that are later than the versions installed on the systems. <p>You can also set one of the following update modes as the default:</p> <ul style="list-style-type: none"> • In-Band (Operating System) — Allows you to update all components on the systems. • Out-of-Band (iDRAC) — Allows you to update only the BIOS, certain firmware, and certain applications. <p> NOTE: You can set one of the update modes as the default mode but the actual update mode depends on the protocol used and the components that are being updated. For more information, see System Update Use Case Scenarios.</p> <p>You can also set your preference to reboot the target server after an update by selecting the After update, if required, reboot the target server option. If this option is selected, the After update, if required, reboot the target server is selected in the System Update Task wizard.</p> <p> NOTE: You can override this preference by selecting or clearing the After update, if required, reboot the target server option in the System Update Task wizard.</p> <p>If After update, if required, reboot the target server option is selected, the Out-of-band Reboot Type option is displayed. This option is disabled by default. Using the Out-of-band Reboot Type option, you can set the types of reboot methods available for the system update. The reboot methods are:</p> <ul style="list-style-type: none"> • Power Cycle (Cold) — Select this option to power off and then restart the system. • Graceful Reboot without forced shutdown (Warm) — Select this option to shut down and then reboot the operating system without forcefully turning off the target system. • Graceful Reboot with forced shutdown (Warm with forced) — Select this option to shut down and then reboot the operating system by forcefully turning off the target system.

Field	Description
	 NOTE: By default, the Graceful Reboot with forced shutdown reboot method is selected.
Systems information — bar chart format	<p>The bar chart lists the following systems:</p> <ul style="list-style-type: none"> Compliant Systems Non-Compliant Systems  NOTE: Non-Inventoried Systems and Issues and Resolutions links are provided below the bar chart. Click these links to navigate to the respective tabs.
Systems information — pie chart format	<p>The pie chart lists the systems status compared with the existing catalog file. The systems listed are as follows:</p> <ul style="list-style-type: none"> Compliant Systems Non-Compliant Systems Non-Inventoried Systems Issues and Resolutions
Compliant Systems	Systems with software that is up to date when compared with versions available in the software updates default catalog. Click compliant systems portion to view more information in the Compliant Systems tab.
Non-Compliant Systems	Systems with software that requires updates when compared with versions available in the software updates default catalog. Click the non-compliant systems portion to view more information in the Non-Compliant Systems tab.
Non-Inventoried Systems	Discovered systems pending inventory when compared with available software in the default catalog. Click non-inventoried portion to view more information in the Non-Inventoried Systems tab.

Compliant Systems

The **Compliant Systems** tab provides this information:

Table 221. Compliant Systems

Field	Description
System Name	Domain name of the system.
Model Type	Devices model information.
Operating System	The operating system that is running on the server.
Service Tag	A unique identifier, that provides the service lifecycle.
Discovered Time	Time and date of discovery.
Inventory Time	Time and date of inventory.
Server Subnet Location	IP address range information.

Non-Compliant Firmware and Drivers

The Non-Compliant Firmware & Drivers tab provides the following information:

Table 222. Non-Compliant Firmware & Drivers

Field	Description
System Name	Domain name of the system.
Group Name	Displays the name of device groups.
Baseline Name	Displays the name of catalog baseline associated with a device group.
Model Type	The systems model name. For example, PowerEdge.
Operating System	The operating system that is installed on the system.
Service Tag	A unique identifier, that provides the service lifecycle information.
Update Method	Displays the update methods such as OpenManage Server Administrator and iDRAC.
Discovered Time	Time and date of discovery.
Inventory Time	Time and date of inventory.

Select noncompliant systems, and select the updates in the **Select Updates to Apply** pane. Click **Apply Selected Updates**.

Table 223. Apply Selected Updates

Field	Description
System Name	System's domain name.
Importance	The requirement of this software update for the system.
Update Method	Displays the update methods such as OpenManage Server Administrator and iDRAC.
Component	The software information.
Type	The type of software update.
Installed Version	The installed version number.
Upgrade/Downgrade	A green arrow indicates an upgrade.
Available Version	The available version number.
Package Name	The name of the software update.
Reboot Required	Specifies whether the update requires a system reboot.




Related link

[System Update](#)

System Update Task

Table 224. System Update Task

Field	Description
Task Name	Provide a name for the software update task.
Select System to Update	Select the system that you want to update.
System Name	Domain name of the system.
Importance	The requirement of this software update for the system.
Delivery Mode	Displays the delivery methods such as OpenManage Server Administrator and iDRAC.

Field	Description
Component	The software information.
Type	The type of software update.
Installed Version	The installed version number.
Upgrade/Downgrade	A green arrow indicates an upgrade.
Available Version	The available version number.
Package Name	The name of the software update.
Reboot required	Indicates if the system must be rebooted after the update.
Set the Task Schedule	
Run Now	Select this option if you want to run the task when you click Finish .
Set Schedule	Select to schedule a task at a required date and time. Click the icon to set date and time.
After update, if required, reboot the target server	Select to restart the system after the software update task is completed.
Out-of-band Reboot Type	<p>Displays the types of reboot methods available for the system update.</p> <p> NOTE: The Out-of-band Reboot Type option is available only if you selected After update, if required, reboot the target server option.</p> <p>Select the reboot method from the following options:</p> <ul style="list-style-type: none"> • Power Cycle (Cold) — Select this option to power off and then restart the system. • Graceful Reboot without forced shutdown (Warm) — Select this option to shut down and then reboot the operating system without forcefully turning off the target system. • Graceful Reboot with forced shutdown (Warm with forced) — Select this option to shut down and then reboot the operating system by forcefully turning off the target system. <p> NOTE: By default, the Graceful Reboot with forced shutdown reboot method is selected.</p>
Skip Signature and Hash Check	Select this option to skip the signature and hash check on the system update package.
Before update, reset the iDRAC	<p>Select this option if you experience failures while performing updates using the iDRAC.</p> <p> CAUTION: Selecting this option may allow the update to succeed, but may also cancel any pending jobs/activities scheduled on the iDRAC.</p>
Enter Credentials for the task execution	
Enable Sudo	Select this option to update the system using sudo.

Field	Description
SSH Port Number	Provide the SSH port number.
Server User name	Provide the server user name for the selected target.
Server Password	Provide the server password for the selected target.
iDRAC User name	Provide the iDRAC user name for the selected target.
iDRAC Password	Provide the iDRAC password for the selected target.

Non-Inventoried Systems

The **Non-Inventoried Systems** tab provides a list of systems that require inventory. To inventory the systems, select the systems and click **Inventory**.

Table 225. Non-Inventoried Systems

Field	Description
System Name	Domain name of the system.
Discovered Time	Time and date of discovery.
Inventory Time	Time and date of inventory.
Server Subnet Location	IP address range information.

Related links

[Updating BIOS, firmware, drivers, and system applications](#)

[Viewing the System Update page](#)

[System Update — Reference](#)

[System Update](#)

Inventory Systems

To inventory systems, select **Systems To Inventory** and click **Run Inventory**.

All System Update Tasks

This page provides more information on the software update tasks.

Table 226. All System Update Tasks

Field	Description
Task Name	The name of the task.
Task Label	Provides information on what the task does.
Start Time	Time and date of inventory.

Related link

[System Update](#)

Issues and Resolutions

Table 227. Issues and Resolutions

Field	Description
System Name	Displays the domain name of the system.
Reason	Displays the issue associated with the server.

Field	Description
Recommendation	Displays the resolution to resolve the issue.

Related links

[Updating BIOS, firmware, drivers, and system applications](#)







[Viewing the System Update page](#)

[System Update — Reference](#)

Task Execution History

Lists the details of the system update tasks or remote tasks.

Table 228. Task Execution History

Field	Description
Status	<p>Displays an icon representing the task status:</p> <ul style="list-style-type: none">  — Running or pending  — Completed  — Stopped  — Failed  — Warning
Task Name	The name of the task.
Start Time	Time and date at which the system update task started.
% Completed	The task's progress information.
Task State	<p>Provides these task states:</p> <ul style="list-style-type: none"> • Running • Completed • Stopped • Failed • Warning <p> NOTE: The task status displays warning if the After update if required, reboot the target server option was not selected for the system update task.</p>
Successful / Attempted Targets	The number of target systems on which the task is successfully executed.
End Time	Time and date at which the system update task ends.
Executed by User	The user information.

Select a Catalog Source

For updating software, select from these options to use a default catalog file present on **downloads.dell.com** or provide an alternate software update package file.

Table 229. Select a Catalog Source

Field	Description
Default Catalog	
Use file system source (SUU)	Select to update software using Server Update Utility. Click Browse to traverse to the file location. The catalog.cab file is located in the repository folder.
Use repository manager file	Select to update software by using Repository Manager file. Click Browse to traverse to file location. The catalog.cab file is located in the repository folder.
Use an online source	Select to update software by using the update package present on downloads.dell.com . Select the online source based on the preferred protocol from the drop-down list.
MX Chassis Default Catalog	
HTTPS	Downloading software update package by using HTTPS. For example, downloads.dell.com/catalog .

 **NOTE:** The path to the catalog file may be displayed on the screen while importing the catalog using either SUU or Repository Manager. However, it is recommended that you manually select the catalog file, by clicking Browse.

Dell Update Package

A Dell Update Package (DUP) is a self-contained executable in a standard package format that updates a single software element on the system. DUPs are software utilities provided by Dell to update specific software components on PowerEdge systems, desktops, and laptops. The customized bundles and repositories are made up of DUPs based on operating systems supported, update types, form factor, and line of business.

OpenManage Server Update Utility

OpenManage Server Update Utility (SUU) is a DVD-based application for identifying and applying updates to the system. SUU displays a comparison report of the versions and provides various options for updating the components.

Repository Manager

Repository Manager is an application that allows you to create repositories of customized bundles and updates, and groups of related updates for systems running supported Microsoft Windows or Linux operating systems. This facilitates generating comparison reports and establishing update baselines of repositories. By using Repository Manager, you can ensure that the PowerEdge system, desktop or laptop is equipped with the latest BIOS, driver, firmware, and software updates.

Viewing the Default Catalog

Select to view the catalog file that is currently in use for applying software updates.

Table 230. View Default Catalog

Field	Description
Source	Displays the source. The source is either Server Update Utility, downloads.dell.com, or Repository Manager.
Source Type	The type for source from which the catalog file is taken. For example, downloads.dell.com.
Release ID	The unique identification number assigned to the released catalog file.
Release Date	The date on which the catalog file was released.

Field	Description
Newer version available	Displays if a newer version is available.

View MX Chassis Default Catalog

Select to view the catalog file that is currently in use for applying firmware and driver updates to the MX7000 chassis including the lead chassis, member chassis, compute sleds, and storage.

Table 231. View MX Chassis Default Catalog

Field	Description
Source	Displays the source. The source is Online for MX7000 chassis.
Source Type	The type for source from which the catalog file is taken.
Release ID	The unique identification number that is assigned to the released catalog file.
Release Date	The date on which the catalog file was released.
Newer version available	Displays if a newer version is available.

View Catalog Baseline Associations

Table 232. View Catalog Baseline Associations

Field	Description
Group Name	Name of the custom device group. By default, PowerEdge MX7000 and VxFlex Ready Nodes groups are also displayed.
Baseline Name	Name of the catalog baseline associated to the custom device group.

List of Catalog Baselines

Table 233. List of Catalog Baselines

Field	Description
Baseline Name	Name of the catalog baseline.
Source	Displays the source. For example, Repository Manager.
Release ID	The unique identification number assigned to the released catalog file.
File Path	File system location of the catalog.
Release Date	The date on which the catalog file was released.

Create Catalog Baseline wizard

Table 234. Create Catalog Baseline wizard

Field	Description
Baseline Name	Name of the catalog baseline.
Use repository manager file	Browse to select the repository manager file.

Baseline Details






Table 235. Baseline Details

Field	Description
Baseline Name	Name of the catalog baseline.
File Path	File system location of the catalog.
Source Type	The type for source from which the catalog file is taken. For example, Custom Catalog.
Release ID	The unique identification number assigned to the released catalog file.
Release Date	The date on which the catalog file was released.

Managing remote tasks

About remote tasks

With the remote tasks feature in OpenManage Essentials, you can:

- Run commands on local and remote systems, run batch files and executable files on the local systems, and schedule local and remote tasks.
-  **NOTE: Ensure that you run the latest commands to successfully execute the remote tasks.**
-  **NOTE: The files must be located on the system with OpenManage Essentials installed and not on the remote system.**
- Change power status for a system.
 - Deploy OpenManage Server Administrator on systems.
 - Deploy iDRAC Service Module on systems.
 - Collect firmware and driver inventory information from a server that does not have OpenManage Server Administrator (OMSA) installed.
 - View the remote tasks.
 - Make changes to any task by right-clicking it.
-  **NOTE: If you stop a running task, it may take 3–4 minutes for the task to stop gracefully and the updated task status to get reflected in the console.**
-  **NOTE: The Task Execution History reflects the remote tasks that you created or deleted only after a few seconds.**
-  **NOTE: When providing system credentials, if the username has spaces or periods, the username must be provided within quotation marks. For example, "localhost\johnny marr" or "us-domain\tim verlaine". Spaces and periods can be used in usernames for OpenMange System Administrator Tasks, Generic Command Line Tasks (local system), OpenManage Systems Administrator Deployment Tasks. System Updates (In Band, through OpenManage System Administrator) also support spaces and periods. Out of Band patching (through RAC device) or commands such as RACADM do not support space or period in the username.**

Managing command line tasks

You can create custom command line tasks to run CLI commands on local and remote systems, and run batch files and executables on local systems.

For example, you can create a custom command line task to run a security audit and gather information about the systems' security status.

-  **NOTE: The Remote Server Administrator Command task requires that the Windows Management Instrumentation service is running on the selected targets.**

To create command line tasks:

1. Click **Manage** → **Remote Tasks** → **Common Tasks** → **Create Command Line Task**.
2. On **General**, enter a task name.
3. Select one of the following options:
 - **Remote Server Administrator Command**—To run the server administrator command on remote servers.
 - **Generic Command**—To run the command, executable file, or batch file.
 - **IPMI Command**—To run the IPMI commands on the remote system.

- **RACADM Command Line**—To run the RACADM commands on the remote system.
4. Based on your selection in the preceding step, provide the following:
 - If you selected **Remote Server Administrator Command**, then enter command, SSH port number, and select **Generate Trusted Key for Linux** if you want to generate a trusted key.
 - If you selected **Generic Command, RACADM Command Line** or **IPMI Command** then enter command and append output information. Providing the append output information is optional.
 5. On **Task Target**, do one of the following:
 - Select a query from the drop-down list, or create a query by clicking the **New** button.
 - Select server targets for running the commands. Only applicable targets are displayed by default. For more information, see [Device Capability Matrix](#).
 6. On **Schedule and Credentials**, enter user credentials, and set schedule for the tasks from available options, and then click **Finish**.
 For information about the fields in the **Create a Command Line Task** wizard, see [Command Line Task](#).

Related links

[Remote Tasks](#)
[Remote Tasks — Reference](#)
[Remote Tasks Home](#)
[Command Line Task](#)
[All Tasks](#)
[Device Capability Matrix](#)

Managing RACADM command line tasks

RACADM command line tasks are used to run commands on remote DRACs and iDRACs. For example, run a RACADM task to configure iDRAC through out of band (OOB) channel. To manage RACADM Command line tasks:

1. Click **Manage** → **Remote Tasks** → **Common Tasks** → **Create Command Line Task**.
2. On **General**, choose **RACADM Command Line** and enter a name for the task.
3. Enter the RACADM subcommand (for example, **getsysinfo**). For a list of RACADM commands, go to Dell.com/support.
4. (Optional) Choose **Output to file** to capture task output from multiple targets. Enter path and filename.
 - To log the information from all selected targets, select **Append**.
 - To write all the detected errors to the log file, select **Include errors**.
5. On **Task Target**, do one of the following:
 - Select a query from the drop-down list, or create a query by clicking the **New** button.
 - Choose target servers or DRACs/iDRACs. Only applicable targets are displayed by default. For more information, see [Device Capability Matrix](#).
6. On **Schedule and Credentials**, set the schedule parameters, enter target credentials and then click **Finish**.

Related links



[Remote Tasks](#)
[Remote Tasks — Reference](#)
[Remote Tasks Home](#)
[Command Line Task](#)
[All Tasks](#)
[Device Capability Matrix](#)

Managing generic command line tasks

Using generic command line task, you can run different types of tasks such as, a batch file, a script file such as a Powershell or VBS script, an executable, or a command, on the local OpenManage Essentials system. While the task always runs on the local OpenManage Essentials system, you can structure the local task to interact with or act upon various remote devices or servers.

You can enter tokens (substitution parameters) in the command line task to be passed to the script file, executable, command, or batch file and execute local scripts on devices that are discovered in OpenManage Essentials.

To manage generic command line tasks:

1. Click **Manage** → **Remote Tasks** → **Common Tasks** → **Create Command Line Task**.
2. In the **General** tab, choose **Generic Command**.
3. If required, update the task name.
4. Enter the path and command (batch, script, or executable) to run on the local system.
5. (Optional) Enter any arguments for the command. If \$USERNAME and \$PASSWORD are used in **Arguments**, you can pass the credentials to the command by the entering the credentials under **Script Credentials**. If \$IP or \$RAC_IP are used in **Arguments**, you can run the command against the selected target(s) by passing the IP address of each target to the command.
 **NOTE: The tokens provided in the Arguments field must entirely be in either uppercase or lowercase. For example, \$HOSTNAME or \$hostname.**
 **NOTE: If you are running a command that does not require any tokens or arguments, the Script Credentials section and the Task Target tab are not displayed.**
6. (Optional) Choose **Ping Device** if you want to ping the device first.
7. (Optional) Choose **Output to file** to capture task output from multiple targets. Enter path and filename.
 - To log the information from all selected targets, select **Append**.
 - To write all the detected errors to the log file, select **Include errors**.
8. On **Task Target**, do one of the following:
 - Select a query from the drop-down list, or create a query by clicking the **New** button.
 - Select targets for running the commands.
9. On **Schedule and Credentials**, enter the local administrator credentials with rights to run commands on the OpenManage Essentials system. Set schedule for the task(s) and then click **Finish**.


Related links

[About tokens](#)

[Generic Command](#)

About tokens

The following tokens can be used to pass values to the batch, script, or executable file:


- **\$IP** and **\$RAC_IP**—If these arguments are used, the **Task Target** tab is displayed in the **Create a Command Link Task** screen. The **Task Target** tab allows you to select the targets to pass the arguments. \$IP is used for a server IP and \$RAC_IP is used for a RAC (iDRAC) IP. From the **Task Target** tab, you can select either groups, a device or use dynamic queries.
- **\$USERNAME** and **\$PASSWORD**—In some instances, you must provide credentials for a remote system in your batch or script file. If \$USERNAME or \$PASSWORD are used in arguments, the **Script Credentials** section is displayed for these values. The credentials entered in the **Script Credentials** section are passed to the command line. You can pass either of these values or both.
 **NOTE: You must enter both values in the Script Credentials section. If you do not need to use one value, enter any text in the field and it is ignored if the token is not in use.**
- **\$NAME**—This token passes the name of the system found in the OpenManage Essentials **Device Tree**. The name is most often the host name of the system, but in some instances it might be either an IP address or a string such as Dell Rack System
– SVCTAG1.

Passing tokens to a script

If you are using a batch file or a script, use %1, %2, %3, and so on, to receive the values passed from OpenManage Essentials. The values are passed in the order they are entered from left to right in the **Arguments** field.

For example, if you use \$USERNAME \$PASSWORD \$IP \$RAC_IP \$NAME as arguments, a batch file with the following Echo %1 %2 %3 %4 %5 displays the following result:

```
C:\Windows\system32>echo scriptuser scriptpw 10.36.1.180 10.35.155.111 M60505-W2K8x64
scriptuser scriptpw 10.36.1.180 10.35.155.111 M60505-W2K8x64
```

 **NOTE:** The credentials are passed in plain text to the command line. If you schedule a task to run later, the credentials are encrypted and stored in the database. The credentials are decrypted when the task runs at the scheduled time. However, if you use the RUN option on a previously created task, enter both administrator credentials for the system and the script credentials.

Managing server power options

You can create tasks to turn on servers.

 **NOTE:** The power task requires that the Windows Management Instrumentation service is running on the selected targets.

To create a remote task:

1. Click **Manage** → **Remote Tasks** → **Common Tasks** → **Create Power Task**.
2. In **Create a Power Task**, on **General**, do the following:
 - a. Enter a task name.
 - b. Select power options. If required, select **Shutdown OS first** to shut down the operating system before starting the power tasks.
3. On **Task Target**, do one of the following:
 - Select a query from the drop-down list, or create a query by clicking the **New** button.
 - Select server targets for running the commands.
4. On **Schedule and Credentials**, set the schedule parameters, enter target credentials, and then click **Finish**.

For information about the fields in the **Create a Power Task** wizard, see [Server Power Options](#).

Related links

[Remote Tasks](#)
[Remote Tasks — Reference](#)
[Remote Tasks Home](#)
[Command Line Task](#)
[All Tasks](#)
[Device Capability Matrix](#)

Deploying OpenManage Server Administrator

The deploy OpenManage Server Administrator task requires the following on the selected targets:

- **Windows Management Instrumentation** service must be running.
- The default **Temp** folder (C:\Users\<username>\AppData\Local\Temp) must be available. Ensure that the **Temp** folder is not deleted or moved.


You can create tasks to deploy OpenManage Server Administrator (OMSA) on servers running Windows or Linux operating systems. You can also plan a date and time to schedule the OMSA deploy task.

To create an OpenManage Server Administrator deployment task:

1. Click **Manage** → **Remote Tasks** → **Common Tasks** → **Create Deployment Task**.
2. On **General**, select **Server Administrator** and enter a task name. If you want to deploy OpenManage Server Administrator on:
 - Windows-based servers—select **Windows**, provide installer path and, if required, provide arguments.
 - Linux-based servers—select **Linux** and provide the installer path and, if required, provide arguments.
 - Select **Generate Trusted Key** and select **Allow reboot**.

For the list of supported packages and arguments (for servers running Window and Linux), see [Supported Windows and Linux Packages](#) and [Arguments](#).

 **NOTE:** Install Server Administrator prerequisites before deploying Server Administrator on Linux.

 **NOTE:** If there are both 32-bit and 64-bit versions of OpenSSL libraries installed on a RHEL system, it is recommended to uninstall the 32-bit version. Also, if there is a symbolic link to `libcrypto.so.6`, created by OpenManage Essentials, remove the symbolic link, and then redeploy OpenManage Server Administrator.

3. On **Task Target**, do one of the following:


- Select a query from the drop-down list, or create a query by clicking the **New** button.
- Select servers on which you want to run this task and click **Next**.

4. On **Schedule and Credentials**, set the schedule parameters, enter user credentials to enable the task.

5. If you want to deploy Server Administrator as a sudo user, select **Enable Sudo** and update the **SSH port** number.

 **NOTE:** Before you deploy OMSA using sudo, create an user account, edit the sudoers file by using the `visudo` command, and add the following:

- For target systems running a 32-bit operating systems: `Cmnd_Alias OMEUPDATE = /bin/tar,/bin/cat,/opt/dell/srvadmin/bin/omexec,/tmp/LinuxPreInstallPackage/runbada,/tmp/LinuxPreInstallPackage/omexec <sudo_username> ALL=OMEUPDATE, NOPASSWD:OMEUPDATE.`
- For target systems running a 64-bit operating systems: `Cmnd_Alias OMEUPDATE = /bin/tar,/bin/cat,/opt/dell/srvadmin/bin/omexec,/tmp/LinuxPreInstallPackage64/runbada,/tmp/LinuxPreInstallPackage64/omexec <sudo_username> ALL=OMEUPDATE, NOPASSWD:OMEUPDATE.`

 **NOTE:** If OMSA is uninstalled from a system by a root user, before deploying OMSA on that system using sudo, make sure that all OMSA preinstallation package files are removed from the tmp folder.

 **NOTE:** Deploying OMSA using sudo is not supported for SUSE Linux Enterprise Server and ESX targets.

6. Click **Finish**.

For information about the fields in the **Create a Deployment Task** wizard, see [Deployment Task](#).


Related links

[Remote Tasks](#)
[Remote Tasks — Reference](#)
[Remote Tasks Home](#)
[Command Line Task](#)
[All Tasks](#)
[Device Capability Matrix](#)

Supported Windows and Linux Packages

Windows Packages

Table 236. Windows Packages

Package Type	Clean installation	Major Version Upgrade (5.x to 6.x to 7.x to 8.x)	Minor Version Upgrade (8.x to 8.y)
.msi	Supported	Supported	Supported
.msp	Not supported	Not supported	Supported
.exe	Not supported	Supported	Supported
 NOTE: OMSA deployment using the .exe package is supported only with Dell Update Packages (DUPs).			

Linux Packages

Table 237. Linux Packages

Operating System	Package
SUSE Linux Enterprise Server 10	OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.SLES10.x86_64_A01.6.tar.gz OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.SLES10.x86_64_A01.6.tar.gz.sign
SUSE Linux Enterprise Server 11	OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.SLES11.i386_A01.14.tar.gz OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.SLES11.i386_A01.14.tar.gz.sign
VMware ESX 4	OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.ESX41.i386_A01.tar.gz OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.ESX41.i386_A01.tar.gz.sign
Red Hat Enterprise Linux 5	OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.RHEL5.x86_64_A01.4.tar.gz OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.RHEL5.x86_64_A01.4.tar.gz.sign
Red Hat Enterprise Linux 6	OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.RHEL6.x86_64_A01.5.tar.gz OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.RHEL6.x86_64_A01.5.tar.gz.sign

Arguments

Clean Installation

Table 238. Clean Installation

Component Installation	Linux Attribute	Windows Attribute
Server Administrator Web Server only	-w	ADDLOCAL=IWS
Server Administrator Instrumentation only	-d	ADDLOCAL=SA
Server Administrator Web Server and Server Instrumentation	-w -d	ADDLOCAL=ALL

Upgrade

- REINSTALL=ALL REINSTALLMODE=VOMUS — This is a required argument for Server Administrator minor version upgrade using .msi packages.
- /qn — This is an optional argument that is used for silent and unattended installation.
-

Deploying iDRAC Service Module

 **NOTE: The iDRAC Service Module can be deployed only on servers that meet the following criteria:**




- PowerEdge 12th generation or later servers running a 64-bit Windows or Linux operating system
- iDRAC firmware version 1.51.51 or later
- The server and iDRAC must be discovered in OpenManage Essentials

The deploy iDRAC Service Module task requires the following on the target servers:



- **Windows Management Instrumentation** service must be running.
- The default **Temp** folder (C:\Users\<username>\AppData\Local\Temp) must be available. Ensure that the **Temp** folder is not deleted or moved.

You can create tasks to deploy the iDRAC Service Module on servers running Windows or Linux operating systems. You can also plan a date and time to schedule the iDRAC Service Module deployment task.

To create an iDRAC Service Module deployment task:

1. Click **Manage** → **Remote Tasks** → **Common Tasks** → **Create Deployment Task**.
2. On **General**, select **iDRAC Service Module** and provide a task name. If you want to deploy the iDRAC Service Module on Windows-based servers, then select **Windows**, provide installer path and, if required, provide arguments. If you want to deploy the iDRAC Service Module on Linux-based servers, select **Linux** and provide the installer path, select **Generate Trusted Key** and **Allow reboot**. If you are using a .rpm package to deploy the iDRAC Service Module, select **Upload and Install GPG key**.
 **NOTE:** Install the iDRAC Service Module prerequisites before deploying the iDRAC Service Module on Linux.
3. On **Task Target**, do one of the following:
 - Select a query from the drop-down list or create a new query by clicking the **New** button.
 - Select servers on which you want to run this task and click **Next**. **NOTE:** Devices that are not applicable for the iDRAC Service Module deployment are not available for selection in the Task Target. Moving the mouse pointer over such a device in the Task Target displays a tool tip that indicates why the iDRAC Service Module cannot be deployed. If you want to override the device capability and allow all the available devices for selection as task targets, select **Enable all**.
4. On **Schedule and Credentials**, set the schedule parameters, provide user credentials to enable the task.
5. If you want to deploy the iDRAC Service Module as a sudo user, select **Enable Sudo** and update the **SSH port** number.
 **NOTE:** Before you deploy the iDRAC Service Module using sudo, create a new user account, edit the sudoers file using the visudo command, and add the following:

```
Cmnd_Alias OMEUPDATE = /bin/tar,/bin/cat,/bin/rpm,/opt/dell/srvadmin/bin/omexec,/tmp/LinuxPreInstallPackage64/runbada,/tmp/LinuxPreInstallPackage64/omexec  
<sudo_username> ALL=OMEUPDATE, NOPASSWD:OMEUPDATE
```

 **NOTE:** If the iDRAC Service Module is uninstalled from a system by a root user, before deploying the iDRAC Service Module on that system using sudo, make sure that all the iDRAC Service Module pre-installation package files are removed from the tmp folder.
 **NOTE:** Deploying the iDRAC Service Module using sudo is not supported on SUSE Linux Enterprise Server and ESX targets.
6. Click **Finish**.

For information about the fields in the **Create a Deployment Task** wizard, see [Deployment Task](#).



Related link

[Deployment Task](#)

Supported Windows and Linux Packages

Windows Packages

Table 239. Windows Packages

Package Type	Clean installation	Major Version Upgrade (1.x to 2.x)
.msi  NOTE: The .msi package is applicable only for deploying iDRAC Service Module version 2.0 or later.	Supported	Supported
.exe  NOTE: iDRAC Service Module deployment using the .exe package is supported only with Dell Update Packages (DUPs).	Not supported	Supported

Linux Packages

Table 240. Linux Packages


Operating System	Package
<ul style="list-style-type: none">Red Hat Enterprise Linux 5Red Hat Enterprise Linux 6Red Hat Enterprise Linux 7SUSE Linux Enterprise Server 11Community Enterprise Operating System (CentOS) 5.9CentOS 6.5	OM-iSM-Dell-Web-LX-100-429.tar.gz OM-iSM-Dell-Web-LX-100-429.tar.gz.sign Systems-Management_Application_NH7WW_LN64_1.0.0_A01 Systems-Management_Application_NH7WW_LN64_1.0.0_A01.BIN
SUSE Linux Enterprise Server 11	dcism-1.0.0-4.435.1.sles11.x86_64.rpm
Red Hat Enterprise Linux 5	dcism-1.0.0-4.435.1.el5.x86_64.rpm
Red Hat Enterprise Linux 6	dcism-1.0.0-4.435.1.el6.x86_64.rpm

Collecting Firmware and Driver Inventory

The **Create F/W & Driver Inventory Task** allows you to collect firmware and driver inventory information from a server. The collected inventory information serves as a baseline that is used by OpenManage Essentials to identify and apply updates on the server. This task allows you to collect firmware and driver inventory information that is otherwise not be available to OpenManage Essentials in the following scenarios:

- Servers discovered using WMI or SSH protocol that do not have OpenManage Server Administrator (OMSA) installed.
- PowerEdge servers or OEM servers that do not have OMSA installed.
- Servers running Linux that have OMSA installed, but the inventory collector component is uninstalled.

After the inventory information is collected, you can update the firmware, BIOS, or drivers of the server through the **System Update** portal.

 **NOTE: The Create F/W & Driver Inventory Task utilizes the inventory collector component to collect firmware and driver inventory from target servers. The inventory collector component is deployed on each target server for collecting the inventory information. After the task is completed, the inventory collector component is automatically removed.**

To collect firmware and driver inventory:

- Perform one of the following:
 - Click **Manage** → **Remote Tasks** → **Create F/W & Driver Inventory Task**.
 - If the server was discovered using WMI/SSH protocol and OMSA is not installed, click **Manage** → **System Update** → **Non-Inventoried Systems**.
 - Select the systems you want to inventory and click **Inventory**.
 - In the **Systems to Inventory** window, click **Run Inventory**.


The **Create a Firmware & Driver Inventory Task** window is displayed.

- On **General**, provide a name for the task.
- If you want to filter the devices to be displayed in the **Task Target** based on the operating system, select **Filter devices based on Operating System**.
 - Select **Windows** or **Linux**.
 - If applicable, select **64-bit System**.

 **NOTE: By default, target devices that have OMSA installed are not displayed on the Task Targets tab.**

- Select **Show OMSA based targets** to also view target devices that have OMSA installed in the **Task Target** tab.

- d. If you selected **Show OMSA based targets**, perform one of the following in the **Future Software Inventory Data Collected by** section:

 **NOTE: The Future Software Inventory Data Collected by options only determine the method OpenManage Essentials utilizes to gather firmware and driver inventory information from target devices after an in-band system update. If the F/W and Driver task based inventory option is selected, scheduled discovery and inventory cycles will still gather the OMSA-based inventory from target devices, except the information in the Software Inventory table.**

- **OMSA based inventory** — Select to revert to gathering firmware and driver inventory information through OMSA on target devices that have OMSA installed.

 **NOTE: To revert to gathering firmware and driver inventory information through OMSA, you must either run the firmware and driver inventory task or delete and rediscover the device.**

- **F/W and Driver task based inventory** — Select to gather firmware and driver inventory information through the inventory collector component, even though OMSA may be installed on the device.

4. On **Task Target**, do one of the following:

- Select a query from the drop-down list or click **New** to create a new query.
- Select servers on which you want to run this task and click **Next**.

5. On **Schedule and Credentials**, set the schedule parameters, provide user credentials to enable the task.

6. Click **Finish**.

The status of the inventory collection is displayed in the **Task Execution History** of the **Remote Tasks** portal.

Related links

[Remote Tasks](#)
[Remote Tasks — Reference](#)
[Remote Tasks Home](#)
[Command Line Task](#)
[All Tasks](#)
[Device Capability Matrix](#)
[Firmware and Driver Inventory Collection Task](#)

Updating the inventory collector component

The **Create F/W & Driver Inventory Task** utilizes the inventory collector component to collect software inventory information from Dell servers. Occasionally, a newer version of the inventory collector component may be available. You can verify if OpenManage Essentials has the latest version of the inventory collector component through the **Dell Solutions** portal. If a newer version of the inventory collector component is available, the **Update** link is displayed on the **Dell Solutions** portal.

To update the inventory collector component:

1. Click **Dell Solutions**.
The **Dell Solutions** portal is displayed.
2. Click the **Update** link displayed in the **Inventory collector component** row.
3. At the confirmation prompt, click **Yes**.

The inventory collector component is downloaded in the background. You can view the status of the update in the **Task Status** grid on the **Home** portal.

Working With Sample Remote Tasks Use Cases

Sample remote tasks are available for Server Power Options, Deploy Server Administrator, and Command Line. Sample remote tasks use cases are disabled by default. To enable a sample use case:

1. Right-click the use case and select **Clone**.
2. Enter the **Cloned Task Name** and click **Ok**.

3. Right-click the cloned task and select **Edit**.
4. Enter the required information and assign targets to the tasks. For information about the options, see [Remote Tasks Reference](#).

Related links

[Remote Tasks](#)
[Remote Tasks — Reference](#)
[Remote Tasks Home](#)
[Command Line Task](#)
[All Tasks](#)
[Device Capability Matrix](#)

Use Cases in Remote Tasks



Server Power Options

Sample-Power On Device—Enable this use case to turn on the server. The system must have RAC/DRAC configured.

Deploy Server Administrator

Sample-OMSA Upgrade Windows—Enable this use case to upgrade OpenManage Server Administrator on a Windows-based system.

Command Line

- **Sample - Windows OMSA Uninstall** — Enable this use case to uninstall OMSA on a system running the Windows Server operating system.
- **Sample - Linux OMSA Uninstall** — Enable this use case to uninstall OMSA on a system running the Linux operating system.
- **Sample - Server XML Configuration** — Enable this use case to apply a specific server configuration to multiple managed nodes. For more information, see [Using the Sample - Server XML Configuration Command Line Task](#).
- **Sample-Generic Command Remote** — Enable this use case to use tokens to receive the IP address or name of inventories systems.
 **NOTE: To use this command, you must enter the local system credentials.**
- **Sample - Generic Command Local** — Enable this use case to run a command or script on system with OpenManage Essentials.
 **NOTE: To use this command, you must enter the local system credentials.**
- **Sample - IPMI Command** — Enable this use case to receive information about the power status of a server.
- **Sample - Remote Command** — Enable this use case to view the system summary through Server Administrator.
- **Sample - RACADM - Clear SEL Log** — Enable this use case to clear the SEL log of RAC.
- **Sample - RACADM-Reset** — Enable this use case to reset the RAC.
- **Sample - RACADM-Lockdown Disable** — Enable this use case to disable lockdown mode of iDRAC9 servers.
- **Sample - Disable Inventory Collector** — Enable this use case to disable the inventory collector on target OMSA servers.
- **Sample - Enable Inventory Collector** — Enable this use case to enable the inventory collector on target OMSA servers.

Firmware and Driver Inventory Task

Scheduled S/W Inventory Task — Enable this use case to collect firmware and driver inventory from a server.

Using the Sample - Server XML Configuration Command Line Task


The following are the prerequisites for using the **Sample - Server XML Configuration** command line task:

- Lifecycle Controller 2 version 1.2 or later
- RACADM version 7.2 or later
- Firmware version 1.30.30 or later
- Express or Enterprise license
- iDRAC7

The **Sample - Server XML Configuration** command line task allows you to apply a specific server configuration to multiple managed nodes. Using Lifecycle Controller 2 version 1.2 or later, a server configuration summary can be exported from an iDRAC in XML format through the “Export Server Configuration” operation.

 **NOTE:** For information on exporting the server configuration summary using Lifecycle Controller 2, see the *Configuration XML Workflows* white paper at DellTechCenter.com/LC.

The server configuration summary XML file can be applied to another iDRAC using the **Sample - Server XML Configuration** command line task.

 **NOTE:** To apply the server configuration summary from one iDRAC to another iDRAC, both the iDRACs must be of the same generation, same license state, and so on. For more information on the requirements, see the *Lifecycle Controller (LC) XML Schema Guide*, *Server Configuration XML File*, and *Configuration XML Workflows* white papers at DellTechCenter.com/LC.

To use the **Sample - Server XML Configuration** command line task:

1. In the OpenManage Essentials **Remote Tasks** portal, right-click the **Sample - Server XML Configuration**, and click **Clone**. The **Input information for the newly cloned task** dialog box is displayed.
2. Provide the **Cloned Task Name** and click **OK**.
3. Right-click the created cloned task and click **Edit**. The **Create a Command Line Task** dialog box is displayed.
4. Edit the **Command** field, and provide the location of the server configuration summary xml file in the OpenManage Essentials management station. For example, set `-f c:\user1\server1.xml-t xml`, where `c:\user1\server1.xml` is the location of the server configuration summary xml file.
5. In the **Targets** tab, select the appropriate targets for applying the server configuration.
6. In the **Schedule and Credentials** tab, select to run or schedule the task, and provide the required credentials.
7. Click **Finish**.

Device Capability Matrix

The following device capability matrix provides information about the type of remote tasks supported on devices that are displayed in the **Task Target** tab.









Table 241. Type Of Remote Tasks Supported On Devices That Are Displayed In The Task Target Tab

Remote Task Type	All Servers (except ESXi) With Server Administrator and Discovered Using SNMP/WMI	Windows-based Servers without Server Administrator and discovered using WMI	Linux-based Servers without Server Administrator and discovered using SSH	DRAC/iDRAC discovered using IPMI	DRAC/iDRAC discovered using SNMP/WS-Man
	DRAC/iDRAC is not discovered			Server operating system is not discovered	
Reboot/power cycle operation	Supported	Supported	Not supported	Not supported	Not supported
Power off operation	Supported	Supported	Not supported	Not supported	Not supported
Power on operation	Not supported	Not supported	Not supported	Supported	Not supported
Remote Server Administrator command task	Supported	Not supported	Not supported	Not supported	Not supported
IPMI command task	Not supported	Not supported	Not supported	Supported	Not supported
RACADM command line task	Not supported	Not supported	Not supported	Not supported	Supported

Remote Task Type	All Servers (except ESXi) With Server Administrator and Discovered Using SNMP/WMI	Windows-based Servers without Server Administrator and discovered using WMI	Linux-based Servers without Server Administrator and discovered using SSH	DRAC/iDRAC discovered using IPMI	DRAC/iDRAC discovered using SNMP/WS-Man
	DRAC/iDRAC is not discovered			Server operating system is not discovered	
Create F/W & Driver Inventory task	Not supported	Supported	Supported	Not supported	Not supported

The following table lists the device discovery requirements for the iDRAC Service Module deployment task. To deploy the iDRAC Service Module, the server and the iDRAC must be discovered using the appropriate protocols specified. For example, to deploy the iDRAC Service Module on a Windows-based server running Server Administrator that is discovered using SNMP/WMI, the iDRAC must be discovered using SNMP/WS-Man.

Table 242. Discovery Requirements for the iDRAC Service Module

Remote Task Type	Server/in-band discovery				iDRAC/out-of-band discovery
	All Windows-based Servers With Server Administrator and Discovered Using SNMP/WMI	All Windows-based Servers With Server Administrator and Discovered Using WMI	Linux-based Servers With Server Administrator and discovered using SNMP/SSH	Linux-based Servers With Server Administrator and discovered using SSH	DRAC/iDRAC discovered using SNMP/WS-Man
iDRAC Service Module deployment task		N/A	N/A	N/A	
	N/A		N/A	N/A	
	N/A	N/A		N/A	
	N/A	N/A	N/A		

Device capabilities for a server or DRAC/iDRAC device are populated during discovery and is leveraged by remote tasks to determine applicable targets for each task type. The capability is populated based on the following parameters:

- Protocol used to discover the server and DRAC/iDRAC. For example, IPMI, SNMP, and so on.
- If Server Administrator is installed on the server.
- Settings enabled on the DRAC/iDRAC.

Selecting the **Enable All** check box allows you to override device capability and allows all the available devices for selection as task targets.

The following device capability matrix provides information about the type of remote tasks supported on devices when the device capabilities are overridden.

Table 243. Type Of Remote Tasks Supported On Devices When The Device Capabilities Are Overridden

Remote Task Type	All Servers (except ESXi) With Server Administrator and Discovered Using SNMP/WMI	Windows-based Servers without Server Administrator and discovered using WMI	Linux-based Servers without Server Administrator and discovered using SSH	DRAC/iDRAC discovered using IPMI	DRAC/iDRAC discovered using SNMP/ WS-Man
	DRAC/iDRAC is not discovered			Server operating system is not discovered	
Reboot/power cycle operation	Supported	Supported	Not supported	Not supported	Not supported
Power off operation	Supported	Supported	Not supported	Not supported	Not supported
Power on operation	Supported if: DRAC/iDRAC information is retrieved and displayed in the inventory page. IPMI over LAN is enabled on the DRAC/iDRAC device. You select Enable All in the Tasks Target tab.	Not supported	Not supported	Supported	Supported if: IPMI over LAN is enabled on the DRAC/iDRAC device. You select Enable All in the Tasks Target tab.
Remote Server Administrator command task		Not supported	Not supported	Not supported	
IPMI command task	Not supported	Not supported	Not supported	Not supported	Not supported
RACADM command line task	Supported if: DRAC/iDRAC information is retrieved and displayed in the inventory page. You select Enable All in the Tasks Target tab.	Not supported	Not supported	Not supported	Supported

 **NOTE:** In the Task Targets tab, if the Enable All option is selected, the iDRAC Service Module deployment is enabled for all discovered servers or unknown devices.

Related links

[Managing command line tasks](#)
[Managing RACADM command line tasks](#)
[Managing server power options](#)
[Deploying OpenManage Server Administrator](#)
[Collecting Firmware and Driver Inventory](#)
[Working With Sample Remote Tasks Use Cases](#)
[Using the Sample - Server XML Configuration Command Line Task](#)
[Deploying iDRAC Service Module](#)
[Remote Tasks](#)
[Remote Tasks — Reference](#)

Remote Tasks — Reference

From Remote Tasks you can:

- Run commands on local and remote systems, batch files and executable files on the local systems, and schedule local and remote tasks.
- Change power status for a system.
- Deploy OpenManage Server Administrator on systems.
- Deploy the iDRAC Service Module on systems.
- Collect firmware and driver inventory.
- View the remote tasks.

Remote Tasks:

- Common Tasks
 - Create Command Line Task
 - Create Deployment Task
 - Create Power Task
 - Create F/W & Driver Inventory Task
- Remote Tasks
 - Server Power Options
 - Deploy Server Administrator
 - Command Line
- F/W & Driver Inventory Task

Related links

[Managing command line tasks](#)
[Managing RACADM command line tasks](#)
[Managing server power options](#)
[Deploying OpenManage Server Administrator](#)
[Collecting Firmware and Driver Inventory](#)
[Working With Sample Remote Tasks Use Cases](#)
[Using the Sample - Server XML Configuration Command Line Task](#)
[Deploying iDRAC Service Module](#)
[Remote Tasks Home](#)
[Command Line Task](#)
[All Tasks](#)
[Device Capability Matrix](#)

Remote Tasks Home

To view Remote Tasks page, in OpenManage Essentials, click **Manage** → **Remote Tasks**.

Related links

- [Managing command line tasks](#)
- [Managing RACADM command line tasks](#)
- [Managing server power options](#)
- [Deploying OpenManage Server Administrator](#)
- [Collecting Firmware and Driver Inventory](#)
- [Working With Sample Remote Tasks Use Cases](#)
- [Using the Sample - Server XML Configuration Command Line Task](#)
- [Deploying iDRAC Service Module](#)
- [Remote Tasks](#)
- [Remote Tasks — Reference](#)

Remote Tasks

Remote Tasks page lists the following information:

- All Tasks
- Server Power Options
- Server Administrator Deployment
- Command Line
- Firmware & Driver Inventory

Related links

- [Managing command line tasks](#)
- [Managing RACADM command line tasks](#)
- [Managing server power options](#)
- [Deploying OpenManage Server Administrator](#)
- [Collecting Firmware and Driver Inventory](#)
- [Working With Sample Remote Tasks Use Cases](#)
- [Using the Sample - Server XML Configuration Command Line Task](#)
- [Deploying iDRAC Service Module](#)
- [Remote Tasks Home](#)
- [Command Line Task](#)
- [All Tasks](#)
- [Device Capability Matrix](#)

All Tasks

Table 244. All Tasks

Field	Description
Scheduled State	Displays if the task is enabled.
Task Name	Names of the task.
Task Label	Type of task that is run, for example; for a command line task the options displayed are Remote Server Administrator Command, Generic Command, IPMI Command, and RACADM Command Line.
Last Run	The last time and date information when the task was run.
Created On	The time and date on which the task was created.
Updated On	The time and date information when the task was run.
Updated By	The name of the user.







Related links

[Managing command line tasks](#)
[Managing RACADM command line tasks](#)
[Managing server power options](#)
[Deploying OpenManage Server Administrator](#)
[Collecting Firmware and Driver Inventory](#)
[Working With Sample Remote Tasks Use Cases](#)
[Using the Sample - Server XML Configuration Command Line Task](#)
[Deploying iDRAC Service Module](#)
[Remote Tasks](#)
[Remote Tasks — Reference](#)

Task Execution History

Lists the details of the system update tasks or remote tasks.


Table 245. Task Execution History


Field	Description
Status	Displays an icon representing the task status:  — Running or pending  — Completed  — Stopped  — Failed  — Warning
Task Name	The name of the task.
Start Time	Time and date at which the system update task started.
% Completed	The task's progress information.
Task State	Provides these task states: <ul style="list-style-type: none">• Running• Completed• Stopped• Failed• Warning  NOTE: The task status displays warning if the After update if required, reboot the target server option was not selected for the system update task.
Successful / Attempted Targets	The number of target systems on which the task is successfully executed.
End Time	Time and date at which the system update task ends.
Executed by User	The user information.

Server Power Options

Select this option to change the power state or restart systems.

Table 246. Server Power Options

Field	Description
General	
Task Name	Provide a name for this server power options task.
Select the type	<p>Select from the following options:</p> <ul style="list-style-type: none"> • Reboot — Restarts the system without powering off. • Power Cycle — Powers off and then restarts the system. <p> NOTE: Make sure that the shutdown option is configured for the operating system before you perform a graceful shutdown using this option. If you use this option without configuring it on the operating system, it restarts the managed system instead of performing a shutdown operation.</p> <ul style="list-style-type: none"> • Power Off — Powers off the system. • Power On — Powers on the system. This option works only on target systems that contain RAC.
Shutdown OS first	Select to shut down the operating system before executing the server power options task.
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click New .
Select the device(s) for this task to target	Select the devices to which you want to assign this task.
Enable All	Select to override the device capability and allow all the available devices for selection as task targets.
Schedule and Credentials	
Set schedule	<p>Select from these options:</p> <ul style="list-style-type: none"> • Activate Schedule — Select this option to activate a schedule for the task. • Run now — Select this option to run the task immediately. • Set schedule — Select this option to set a date and time for the task to run. • Run Once — Select this option to run the task on the planned schedule only once. • Periodic — Select this option to run the task frequently at specified intervals: <ul style="list-style-type: none"> – Hourly — Select this option to run the task once every hour. – Daily — To run the task once every day. – Weekly — To run the task once every week. – Monthly — To run the task once every month. <p>Range of Recurrence:</p> <ul style="list-style-type: none"> • Start — To specify the date and time at which the task should begin. • No End Date — To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. • End By — To stop the task at the specified date and time.
Enter User Name and Password	User Name — Provide in the format domain\user name or local host\user name.

Field	Description
	<p>Password — Provide the password.</p> <p>Power On works only on target systems with iDRAC; use the IPMI credentials to perform Power On task.</p> <p>If you selected Power On, then provide the KG key.</p> <p>KG Key — Enter the KG Key. DRAC also supports IPMI KG Key. Each BMC is configured to require an access key in addition to user credentials. The KG key is prompted only for power-on task and not other power tasks because it is an IPMI task.</p> <p> NOTE: The KG key is a public key that is used to generate an encryption key for use between the firmware and the application; and is available only on PowerEdge 9G and later systems. The KG key value is an even number of hexadecimal characters. In the format, yxxx, y denotes alphanumeric characters and x denotes numbers.</p>

Related links

[Managing server power options](#)




[Device Capability Matrix](#)

Deployment Task

Select this option to create tasks to deploy either Server Administrator or iDRAC Service Module on selected servers.

Table 247. Deployment Task

Field	Description
General	
Deployment Type	<p>Select the type of deployment from the following options:</p> <ul style="list-style-type: none"> • Server Administrator • iDRAC Service Module
Task Name	Provide a name for the task.
Select the type	<p>Select from the target type from the following options:</p> <ul style="list-style-type: none"> • Windows • Linux
Installer Path	<p>The location where the Server Administrator or iDRAC Service Module installer is available.</p> <p>For Windows, packages with .dup, .msi, and .msp file extensions are available. Msi packages enable Server Administrator installation and upgrades while dup and msp packages enable only Server Administrator upgrades.</p> <ul style="list-style-type: none"> • For Server Administrator deployment on Linux: <ul style="list-style-type: none"> – Packages with the tar.gz file extensions are available. – The .sign file is required for verification. The .sign file must be available in the same folder as the tar.gz file. • For the iDRAC Service Module deployment on Linux: <ul style="list-style-type: none"> – Packages with the tar.gz, .rpm and .bin file extensions are available.

Field	Description
	<ul style="list-style-type: none"> For deploying the .rpm file, the RPM-GPG-KEY file must be available in the same folder as the .rpm file.
Install Arguments  NOTE: Applicable only for Server Administrator deployment task.	(Optional) Provide arguments. For example, in Windows, the parameters are as follows: <ul style="list-style-type: none"> ADDLOCAL = IWS — Server Administrator web server only ADDLOCAL = SSA — Server instrumentation only For example, in Linux, the parameters are as follows: <ul style="list-style-type: none"> -w — Server administrator web server only -d — Server instrumentation only See the <i>Dell OpenManage Installation and Security User's Guide</i> at Dell.com/support for a complete list of arguments.
Generate Trusted Key	This option is available if you selected Linux. Select this option to generate a trusted key.
64-bit System	Select this option if you are deploying the 64-bit version of Server Administrator on a managed node.
Allow reboot (if required)	Select this option to restart the server once you deploy Server Administrator on the server.
Upload and Install GPG key (requires GPG key in same folder)  NOTE: Applicable only for the iDRAC Service Module deployment task.	This option is available if you select a .rpm file for the iDRAC Service Module deployment. Select this option to validate the .rpm file on the target device.
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click New .
Select server(s) for this task to target	Select the servers to which you want to assign this task.
Enable all  NOTE: Applicable only for the iDRAC Service Module deployment task.	Select to override the device capability and display all the available devices for selection as task targets.
Schedule and Credentials	
Set schedule	Select from these options: <ul style="list-style-type: none"> Activate Schedule — Select this option to activate a schedule for the task. Run now — Select this option to run the task immediately. Set schedule — Select this option to set a date and time for the task to run.
Enter credentials of remote target(s)	
User Name	Provide in the format domain\user name or local host\user name.
Password	Provide the password.
Enable Sudo	Select this option to deploy Server Administrator or the iDRAC Service Module using Sudo.
SSH Port	Provide the SSH port number.

Related links

[Deploying OpenManage Server Administrator](#)
[Device Capability Matrix](#)

Command Line Task

Select this option to create command line tasks.

Table 248. Command Line Task

Field	Description
Task Name	Provide name of the task.
Remote Server Administrator Command	Select this option to run Remote Server Administrator Command on selected servers.
Generic Command	Select this option to run executable and commands on the system with OpenManage Essentials.
IPMI Command	Select this option to run IPMI commands on selected servers.
RACADM Command Line	Select this option to run RACADM commands on selected servers.


Related links

[Managing command line tasks](#)
[Managing RACADM command line tasks](#)
[Managing server power options](#)
[Deploying OpenManage Server Administrator](#)
[Collecting Firmware and Driver Inventory](#)
[Working With Sample Remote Tasks Use Cases](#)
[Using the Sample - Server XML Configuration Command Line Task](#)
[Deploying iDRAC Service Module](#)
[Remote Tasks](#)
[Remote Tasks — Reference](#)
[Remote Server Administrator Command](#)
[Generic Command](#)
[IPMI Command](#)
[RACADM Command Line](#)

Remote Server Administrator Command

Table 249. Remote Server Administrator Command

Field	Description
Command	Provide command, for example, <code>omereport system summary</code> .
Ping Device	This option performs a ping test to verify if a device is reachable before it runs a task against it. This option can be used when using \$IP or \$RAC_IP and it decreases the time it takes to run the task(s) as it skips unreachable devices.
Output to file	Select to enable output to a log file. This option captures standard output and writes it to the log file. If you select this option, enter the path name and file name of the log file. This option is disabled by default.
Append	Select to append output from the completed command to the specified file. If the file does not exist, it is created.

Field	Description
Include errors	Select to write all OpenManage Essentials-detected errors to the log file. For example, if no response is received to a ping request before the execution of the command, an error is written to the log file.
SSH Port number	Provide the Secure Shell (SSH) port number on the managed Linux system. The default value for the port number is 22.
Generate Trusted Key for Linux	<p>Select this option to generate a trusted device key for communicating with devices. This option is disabled by default.</p> <p> NOTE: The first time that OpenManage Essentials communicates with a managed device with Linux operating system, a key is generated and stored on both the devices. This key is generated per device and enables a trust relationship with the managed device.</p>
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click New .
Select the server(s) for this task target	Select the servers to which you want to assign this task.
Enable All	Select to override the device capability and allow all the available devices for selection as task targets.
Schedule and Credentials	
Set schedule	<p>Select from these options:</p> <ul style="list-style-type: none"> • Activate Schedule—Select this option to activate a schedule for the task. • Run now—Select this option to run the task immediately. • Set schedule—Select this option to set a date and time for the task to run. • Run Once—Select this option to run the task on the planned schedule only once. • Periodic—Select this option to run the task frequently at specified intervals. <ul style="list-style-type: none"> – Hourly—Select this option to run the task once every hour. – Daily—To run the task once every day. – Weekly—To run the task once every week. – Monthly—To run the task once every month. <p>Range of Recurrence:</p> <ul style="list-style-type: none"> • Start—To specify the date and time at which the task should begin. • No End Date—To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. • End By—To stop the task at the specified date and time.
Enter credentials of the remote target(s)	<p>User Name—Provide in the format domain\user name or local host\user name.</p> <p>Password—Provide the password.</p>

Related links

[Command Line Task](#)

[Managing command line tasks](#)

[Using the Sample - Server XML Configuration Command Line Task](#)

Generic Command

Table 250. Generic Command

Field	Description
Task Name	Enter a name for the task. By default, the task name is populated in the format: <code><task name>-<date and time></code> .
Command	Provide the fully qualified path name and file name of the executable, command, or script file that launches the application program. For example: <ul style="list-style-type: none">• Tracert• C:\scripts\trace.bat• D:\exe\recite.exe
Arguments	Enter command line switches to a command or executable or pass values to a script or batch file. For example, -4 \$IP. If this argument is passed to tracert command, it executes IPV4 only Traceroute against the IPs of servers selected in Task Target tab. The command run would be <code>tracert -4 10.35.0.55</code> . For more information, see About Tokens .
Ping Device	This option performs a ping test to verify if a device is reachable before it runs a task against it. This option can be used when using \$IP or \$RAC_IP and it decreases the time it takes to run the task(s) as it skips unreachable devices.
Output to file	Select to enable output to a log file. This option captures standard output from the running application and writes it to the log file. If you select this option, you must enter the path name and file name of the log file. This option is disabled by default.
Append	Select this option to continue writing to the same file if you run a task multiple times.
Include errors	Select to write all OpenManage Essentials-detected errors to the log file. For example, if no response is received to a ping request before the execution of the command, an error is written to the log file.
Schedule and Credentials	
Set schedule	Select from these options: <ul style="list-style-type: none">• Activate Schedule — Select this option to activate a schedule for the task.• Run now — Select this option to run the task immediately.• Set schedule — Select this option to set a date and time for the task to run.• Run Once — Select this option to run the task on the planned schedule only once.• Periodic — Select this option to run the task frequently at specified intervals.<ul style="list-style-type: none">– Hourly — Select this option to run the task once every hour.

Field	Description
	<ul style="list-style-type: none"> – Daily — To run the task once every day. – Weekly — To run the task once every week. – Monthly — To run the task once every month. <p>Range of Recurrence:</p> <ul style="list-style-type: none"> • Start — To specify the date and time at which the task should begin. • No End Date — To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. • End By — To stop the task at the specified date and time.
Enter the credentials with appropriate privileges to run this task on this system	<p>User Name — Provide OpenManage Essentials user credentials in the format domain\user name or local host\user name.</p> <p>Password — Provide the password.</p>

Related links

[Command Line Task](#)


[Managing command line tasks](#)

[Using the Sample - Server XML Configuration Command Line Task](#)

IPMI Command

Table 251. IPMI Command

Field	Description
Command	Provide the IPMI command you want to run on selected targets.
Ping Device	This option performs a ping test to verify if a device is reachable before it runs a task against it. This option can be used when using \$IP or \$RAC_IP and it decreases the time it takes to run the task(s) as it skips unreachable devices.
Output to file	Select to enable output to a log file. This option captures standard output from the running application and writes it to the log file. If you select this option, enter the path name and file name of the log file. This option is disabled by default.
Append	Select to append output from the completed command to the specified file. If the file does not exist, it is created.
Include errors	Select to write all OpenManage Essentials-detected errors to the log file. For example, if no response is received to a ping request before the execution of the command, an error is written to the log file.
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click New .
Select server(s) for this task to target	Select the servers to which you want to assign this task.
Enable All	Select to override the device capability and allow all the available devices for selection as task targets.
Schedule and Credentials	
Set schedule	Select from these options:

Field	Description
	<ul style="list-style-type: none"> • Activate Schedule — Select this option to activate a schedule for the task. • Run now — Select this option to run the task immediately. • Set schedule — Select this option to set a date and time for the task to run. • Run Once — Select this option to run the task on the planned schedule only once. • Periodic — Select this option to run the task frequently at specified intervals. <ul style="list-style-type: none"> – Hourly — Select this option to run the task once every hour. – Daily — To run the task once every day. Weekly — To run the task once every week. – Monthly — To run the task once every month. <p>Range of Recurrence:</p> <ul style="list-style-type: none"> • Start — To specify the date and time at which the task should begin. • No End Date — To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. • End By — To stop the task at the specified date and time.
Enter Remote Access Controller credentials for target(s)	
User Name	The RACADM task requires IPMI credentials. Provide IPMI credentials to run the task.
Password	Provide the password.
KG key	<p>Enter the KG key value. DRAC also supports IPMI KG key value. Each BMC or DRAC is configured to require an access key in addition to user credentials.</p> <p> NOTE: The KG key is a public key that is used to generate an encryption key for use between the firmware and the application. The KG key value is an even number of hexadecimal characters.</p>

Related links

[Command Line Task](#)
[Managing command line tasks](#)
[Using the Sample - Server XML Configuration Command Line Task](#)

RACADM Command Line

Table 252. RACADM Command Line

Field	Description
Command	Provide the RACADM command you want to run on the servers.
Ping Device	This option performs a ping test to verify if a device is reachable before it runs a task against it. This option can be used when using \$IP or \$RAC_IP and it decreases the time it takes to run the task(s) as it skips unreachable devices.
Output to file	Select to enable output to a log file. This option captures standard output from the running application and writes it to the

Field	Description
	log file. If you select this option, you must enter the path name and file name of the log file. This option is disabled by default.
Append	Select to append output from the completed command to the specified file. If the file does not exist, it is created.
Include errors	Select to write all OpenManage Essentials-detected errors to the log file. For example, if no response is received to a ping request before the execution of the command, an error is written to the log file.
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click New .
Select the server(s) for this task to target	Select the servers to which you want to assign this task.
Enable All	Select to override the device capability and allow all the available devices for selection as task targets.
Schedule and Credentials	
Set schedule	<p>Select from these options:</p> <ul style="list-style-type: none"> • Activate Schedule — Select this option to activate a schedule for the task. • Run now — Select this option to run the task immediately. • Set schedule — Select this option to set a date and time for the task to run. • Run Once — Select this option to run the task on the planned schedule only once. • Periodic — Select this option to run the task frequently at specified intervals. <ul style="list-style-type: none"> – Hourly — Select this option to run the task once every hour. – Daily — To run the task once every day. – Weekly — To run the task once every week. – Monthly — To run the task once every month. <p>Range of Recurrence:</p> <ul style="list-style-type: none"> • Start — To specify the date and time at which the task should begin. • No End Date — To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. • End By — To stop the task at the specified date and time.
Enter Remote Access Controller credentials for target(s)	<p>User Name — The RACADM task requires IPMI credentials. Provide IPMI credentials to run the task.</p> <p>Password — Provide the password.</p>

Related links

[Command Line Task](#)

[Managing command line tasks](#)

[Using the Sample - Server XML Configuration Command Line Task](#)

Firmware and Driver Inventory Collection Task

Select this option to collect firmware and driver inventory information from a server that does not have OpenManage Server Administrator installed.

Table 253. Firmware and Driver Inventory Collection Task

Field	Description
General	
Task Name	Provide a name for the inventory collection task.
Filter devices based on operating system	Select to filter devices to be displayed in the Task Target based on the selected operating system.
Select the Operating System	Select from the following options: <ul style="list-style-type: none"> • Windows • Linux
64-bit System	Select this option if the target server is running a 64-bit operating system.
Show OMSA based targets	Select to display devices from which inventory is currently gathered through OMSA in the Task Target tab.
Future Software Inventory Data Controlled by:	Select from the following options: <ul style="list-style-type: none"> • OMSA based inventory — Select to use OMSA to gather inventory information from the target devices. • F/W and Driver task based inventory — Select to use the inventory collector component to gather inventory information from the target devices.
Task Target	
Select a query	Select a query from the drop-down list. To create a new query, click New .
Select the servers(s) for this task to target	Select the servers you want to assign the task.
Schedule and Credentials	
Set schedule	Select from these options: <ul style="list-style-type: none"> • Activate Schedule — Select this option to activate a schedule for the task. • Run now — Select this option to run the task immediately. • Set schedule — Select this option to set a date and time to run the task. • Run Once — Select this option to run the task on the planned schedule only once. • Periodic — Select this option to run the task frequently at specified intervals: <ul style="list-style-type: none"> – Hourly — Select this option to run the task once every hour. – Daily — Select this option to run the task once every day. – Weekly — Select this option to run the task once every week. – Monthly — Select this option to run the task once every month. <p>Range of Recurrence:</p>

Field	Description
	<ul style="list-style-type: none"> • Start — To specify the date and time at which the task should begin. • No End Date — To continuously run this task based on the selected frequency. For example, if you selected Hourly, then this task continuously runs every hour from the start time. • End By — To stop the task at the specified date and time.
Enter credentials of the remote targets	<p>User Name — Provide in the format domain\user name or local host\user name.</p> <p>Password — Provide the password.</p>

Related link

[Collecting Firmware and Driver Inventory](#)

Managing security settings

Using security roles and permissions

OpenManage Essentials provides security through role-based access control (RBAC), authentication, and encryption. RBAC manages security by determining the operations run by persons in particular roles. Each user is assigned one or more roles, and each role is assigned one or more user rights that are permitted to users in that role. With RBAC, security administration corresponds closely to an organization's structure.

OpenManage Essentials roles and associated permissions are as follows:

- **OmeUsers** have limited access and rights and can perform read-only operations in OpenManage Essentials. They can log in to the console, run discovery and inventory tasks, view settings, and acknowledge events. The Windows Users group is a member of this group.
- **OmeAdministrators** have full access to all the operations within OpenManage Essentials. Windows Administrators group is member of this group.
- **OmeSiteAdministrators** have full access to all the operations within OpenManage Essentials with the following rights and restrictions:
 - Can only create custom device groups under **All Devices** in the device tree. They can create remote or system update tasks on the custom device groups only after the custom device groups are assigned to them by the **OmeAdministrators**.
 - Cannot edit custom device groups.
 - Can delete custom device groups.
 - Can create remote and system update tasks on only the device groups assigned to them by the **OmeAdministrators**.
 - Can only run and delete remote and system update tasks that they have created.
 - Cannot edit remote tasks, including activating or deactivating the task schedule.
 - Cannot clone remote or system update tasks.
 - Can delete tasks they have created.
 - Can delete devices.
 - Cannot edit or target device queries.
 - Cannot edit or access the **Device Group Permissions** portal.
 - Cannot create remote and system update tasks based on a device query.
 - Can create compute pools with devices to which they have permissions.
 - Can perform bare metal and stateless deployments with devices to which they have permissions.
 - Can only edit, rename, unlock, and delete compute pools to which they have permissions.
 - Can only replace a server within a compute pool to which they have permission.
 - Can only reclaim identities from devices included in the compute pool to which they have permission.



NOTE: Any changes made to the role or device group permissions of a user are effective only after the user logs out and logs in again.

- **OmePowerUsers** have the same rights as **OmeAdministrators** except that they cannot edit the settings of OpenManage Essentials.

Microsoft Windows authentication

For supported Windows operating systems, OpenManage Essentials authentication is based on the operating system's user authentication system using Windows NT LAN Manager (NTLM v1 and NTLM v2) modules. For the network, this underlying authentication system allows you to incorporate OpenManage Essentials security in an overall security scheme.

Assigning user rights

You do not have to assign user rights to OpenManage Essentials users before installing OpenManage Essentials. The following procedures provide step-by-step instructions for creating OpenManage Essentials users and assigning user rights for Windows operating system.

 **NOTE: Log in with administrator rights to perform these procedures.**

 **NOTE: For questions about creating users and assigning user group rights or for more detailed instructions, see the operating system documentation.**

1. From Windows desktop, click **Start** → **All Programs** → **Administrative Tools** → **Computer Management**.
2. In the console tree, expand **Local Users and Groups**, and click **Groups**.
3. Double-click either the **OmeAdministrators**, **OMEPowerUsers**, or **OmeUsers** group to add the new user.
4. Click **Add** and type the user name that you are adding. Click **Check Names to validate** and then click **OK**.

New users can log on to OpenManage Essentials with the user rights for their assigned group.

Using Custom SSL Certificates—Optional

OpenManage Essentials default settings ensure that a secure communication is established within your environment. However, some users may prefer to utilize their own SSL certificate for encryption.

To create a new domain certificate:

1. Open Internet Information Services (IIS) Manager by clicking **Start** → **All Programs** → **Administrative Tools** → **Internet Information Services (IIS) Manager**.
2. Expand the <server name> and click **Server Certificates** → **Sites**.
3. Click **Create Domain Certificate** and enter the required information.

 **NOTE: All systems display a certificate error until the domain administrator has published the certificate to the clients.**

Configuring IIS Services

To use a custom SSL certificate, you must configure IIS Services on the system where OpenManage Essentials is installed.

1. Open Internet Information Services (IIS) Manager by clicking **Start** → **All Programs** → **Administrative Tools** → **Internet Information Services (IIS) Manager**.
2. Expand the <server name> → **Sites**.
3. Right-click **DellSystemEssentials** and select **Edit Bindings**.
4. In **Site Bindings**, select the **https binding** and click **Edit**.
5. In **Edit Site Binding**, from the **SSL certificate** drop-down list select your custom SSL certificate and click **OK**.

Supported protocols and ports in OpenManage Essentials

Supported protocols and ports on management stations

Table 254. Supported protocols and ports on management stations

Port number	Protocol	Port type	Maximum encryption level	Direction	Usage
21	FTP	TCP	None	In/Out	Access downloads.dell.com
25	SMTP	TCP	None	In/Out	Optional email alert action
162	SNMP	UDP	None	In	Event reception through SNMP
445	SMB	TCP	None	In/Out	Server configuration and deployment
1278	HTTP	TCP	None	In/Out	Web GUI; downloading packages to Lifecycle Controller
1279	Proprietary	TCP	None	In/Out	Scheduling tasks
1433	Proprietary	TCP	None	In/Out	Optional remote SQL Server access
2606	Proprietary	TCP	None	In/Out	Network monitoring
2607	HTTPS	TCP	128-bit SSL	In/Out	Web GUI
3355	Proprietary	TCP	None	In/Out	Optional OpenManage Mobile push notifications

Supported protocols and ports on managed nodes

Table 255. Supported protocols and ports on managed nodes

Port number	Protocol	Port type	Maximum encryption level	Direction	Usage
22	SSH	TCP	128 bit	In/Out	Contextual application launch — SSH client Remote software updates to Server Administrator —for systems supporting Linux operating systems Performance monitoring in Linux systems.
80	HTTP	TCP	None	In/Out	Contextual application launch — Networking console.
135	RPC	TCP	None	In/Out	Event reception through CIM from Server Administrator — for systems supporting Windows operating systems. Remote software update transfer to Server Administrator—for systems supporting Windows operating systems Remote Command Line— for systems supporting Windows operating systems.
161	SNMP	UDP	None	In/Out	SNMP query management.
623	RMCP	UDP	None	In/Out	IPMI access through LAN.
1311	HTTPS	TCP		In/Out	Contextual application launch — OMSA.
1443	Proprietary	TCP	None	In/Out	Optional remote SQL Server access.

Port number	Protocol	Port type	Maximum encryption level	Direction	Usage
443	Proprietary/WSMAN	TCP	None	In/Out	EMC storage, iDRAC6, iDRAC7, and iDRAC8 discovery and inventory.
2463	Proprietary	TCP	None	From OpenManage Essentials to the managed node	Discovery and inventory of PowerVault MD storage array
3389	RDP	TCP	128-bit SSL	In/Out	Contextual application launch — Remote desktop to Windows terminal services.
5900–5901	Proprietary	TCP	None	In/Out	iDRAC virtual media service.
5900–5901	Proprietary	TCP	None	In/Out	iDRAC console redirection.
6389	Proprietary	TCP	None	In/Out	Enables communication between a host system (through NaviCLI/NaviSec CLI or Navisphere host agent) and a Navisphere Array Agent on a Storage system.

 **NOTE:** For more information about the protocols and ports, visit DellTechCenter.com/OME.

Supported Protocols and Ports on Management Stations

Table 256. Supported Protocols and Ports on Management Stations

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
21	FTP	TCP	None	In/Out	Access ftp.dell.com
25	SMTP	TCP	None	In/Out	Optional e-mail alert action
162	SNMP	UDP	None	In	Event reception through SNMP
445	SMB	TCP	None	In/Out	Server configuration and deployment
1278	HTTP	TCP	None	In/Out	Web GUI; downloading packages to Lifecycle Controller
1279	Proprietary	TCP	None	In/Out	Scheduling tasks
1433	Proprietary	TCP	None	In/Out	Optional remote SQL Server access
2606	Proprietary	TCP	None	In/Out	Network monitoring
2607	HTTPS	TCP	128-bit SSL	In/Out	Web GUI

Supported Protocols and Ports on Managed Nodes

Table 257. Supported Protocols and Ports on Managed Nodes

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
22	SSH	TCP	128 bit	In/Out	Contextual application launch — SSH client Remote software updates to Server Administrator —for systems supporting Linux operating

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
					systems Performance monitoring in Linux systems.
80	HTTP	TCP	None	In/Out	Contextual application launch — Networking console.
135	RPC	TCP	None	In/Out	Event reception through CIM from Server Administrator — for systems supporting Windows operating systems. Remote software update transfer to Server Administrator—for systems supporting Windows operating systems Remote Command Line—for systems supporting Windows operating systems.
161	SNMP	UDP	None	In/Out	SNMP query management.
623	RMCP	UDP	None	In/Out	IPMI access through LAN.
1311	HTTPS	TCP		In/Out	Contextual application launch — OMSA.
1443	Proprietary	TCP	None	In/Out	Optional remote SQL Server access.
443	Proprietary/ WSMAN	TCP	None	In/Out	EMC storage, iDRAC6, iDRAC7, and iDRAC8 discovery and inventory.
2463	Proprietary	TCP	None	From OpenManage Essentials to the managed node	Discovery and inventory of PowerVault MD storage array
3389	RDP	TCP	128-bit SSL	In/Out	Contextual application launch — Remote desktop to Windows terminal services.
5900–5901	Proprietary	TCP	None	In/Out	iDRAC virtual media service.
5900–5901	Proprietary	TCP	None	In/Out	iDRAC console redirection.
6389	Proprietary	TCP	None	In/Out	Enables communication between a host system (through NaviCLI/NaviSec CLI or Navisphere host agent) and a Navisphere Array Agent on a Storage system.

Dell EMC OpenManage Framework

The following illustration provides an overview of the network connections between various components.

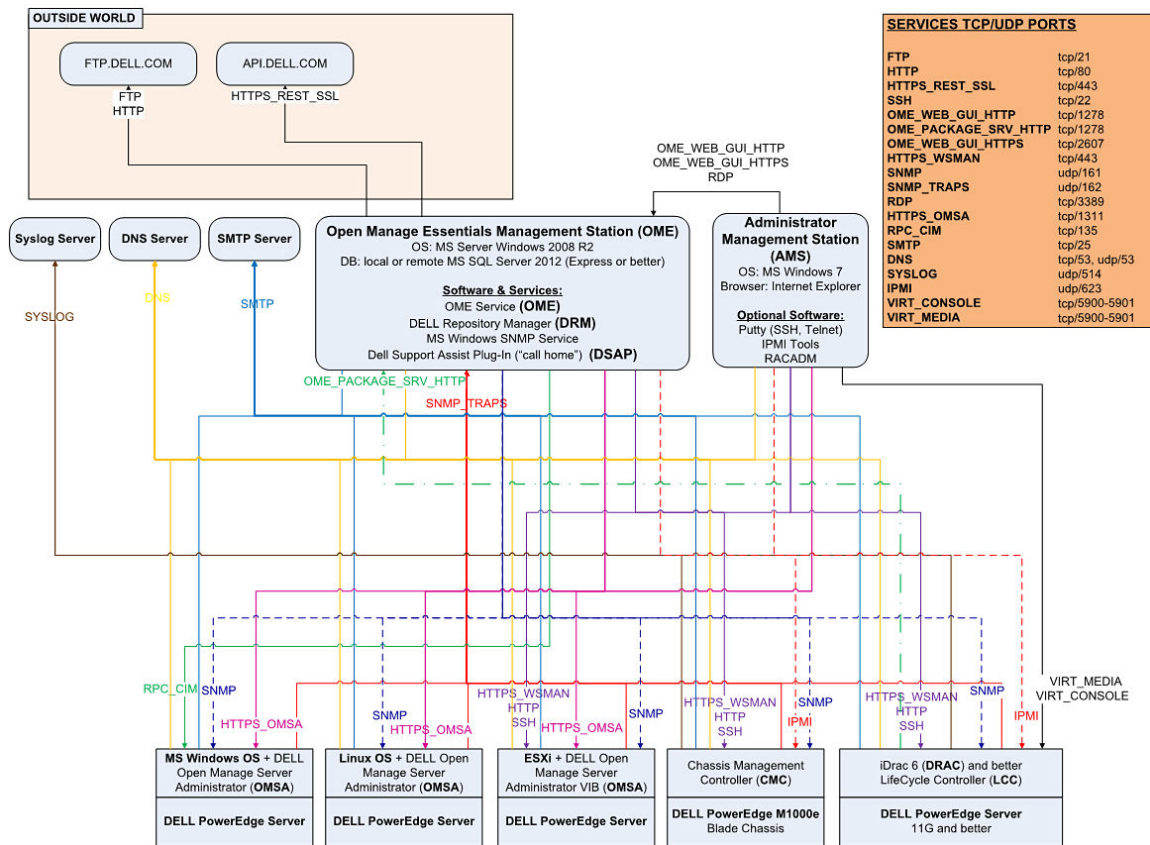


Figure 35. Network Connections

Troubleshooting

OpenManage Essentials Troubleshooting Tool

The OpenManage Essentials troubleshooting tool is a standalone tool that installs along with OpenManage Essentials. You can use the troubleshooting tool for a wide array of protocol related problems that are often at the root of discovery and alert issues.

This tool provides the following protocol-specific diagnostics to identify the problem with the remote node:

- Database—Fetches all the user defined databases present on the remote box.
- Dell EMC—Verifies the connection to the Dell EMC storage devices.
- ICMP—Verifies whether you can ping the remote device from the local box.
- IPMI—Verifies the IPMI protocol to connect to BMC/iDRAC.
- Name Resolution—Verifies whether you can get the resolved name from the local box.
- OpenManage Server Administrator Remote Enablement—This test helps you to verify that OpenManage Server Administrator's remote enablement feature is working on the managed node (OpenManage Server administrator installed with the remote enablement component). This tool behaves like a Server Administrator Distributed Web server (DWS) and connects to Server Administrator managed node instrumentation agent using the WSMAN protocol.

To connect successfully, the Managed Node must have OpenManage Server Administrator installed with the Remote Enablement feature working.

- Port—Verifies whether managed node is listening to the specified port. You can specify 1-65,535 port numbers.
- PowerVault Modular Disk Arrays—Verifies that PowerVault modular disk storage array protocol is used to connect to PowerVault Storage devices.
- Services—Uses SNMP protocol to fetch the running services on the managed node.
- SNMP—Verifies SNMP connection to the remote node, using the required SNMP community string, retries, and time out. First it tries to connect to MIB-II agent and then various other agents to find out the type of device. Troubleshooting Tool also gathers other agent specific information from that device.
- SSH—Verifies that the SSH protocol is used to connect to managed node.
- WMI—Verifies WMI/CIM connection to the remote node. Default retries and time out values are used internally.
- WSMAN—Attempts to connect to WSMAN client on the remote node. Use this test to verify connectivity problems with iDRAC, ESX, and other devices, which support WSMAN specification. This test will connect to such devices and will also list the exposed WSMAN profiles enabled on the remote device.

Troubleshooting Procedures

Troubleshooting Inventory

Inventoried Linux servers are listed under Non-Inventoried systems, numerous retries does not resolve this.

To resolve this issue for the Red Hat Enterprise Linux 5.5, SUSE Linux Enterprise Server version 10 and version 11 installed servers:

1. Mount the *Systems Management Tools and Documentation DVD* (version 6.5 or later) on the Linux server.
2. Install **srvadmin-cm** rpm.
3. Restart OpenManage Server Administrator 6.5.
4. Make sure the OpenManage Server Administrator inventory collector is working from the location **/opt/dell/srvadmin/sbin/invcol**, run **/invcol -outc=/home/inv.xml**.
5. Perform server inventory.

Troubleshooting Device Discovery

If a device discovery is not successful, perform the following steps to troubleshoot and fix the problem:

1. If the device assigned for discovery is a PowerEdge system, ensure that OpenManage Server Administrator is installed on it.
2. To discover Windows devices successfully, configure the SNMP services appropriately. For detailed information on configuring SNMP services on Windows, see [Configuring SNMP Services on Windows](#).
3. To discover Linux devices successfully, configure the SNMP services appropriately. For detailed information on configuring SNMP services on Linux, see [Configuring SNMP Services on Linux](#).
4. After configuring the SNMP services, verify whether the SNMP services are responding correctly.
5. If the device assigned for discovery is Microsoft Windows and you want to use WMI, ensure that the user name and password used in the WMI credentials has the local administrator permissions on the machine that you want to discover. You can use the Microsoft **wbemtest** utility to ensure that WMI connectivity to the Windows Server is correct.
6. If the device assigned for discovery is a non-server network device, such as a printer, Networking Ethernet switch, and so on, ensure that SNMP is enabled on the device. You can do this by accessing the Web interface for a device.
7. If there are changes in the IP address or FQDN for the target devices, in a DNS environment, then OpenManage Essentials will not display the correct IP Address and device names (FQDN) on the console. You must wait for the Operating System to update the DNS cache on the console, or run **ipconfig /flushdns** to flush the DNS cache, and then re-run the discovery and inventory tasks on the affected discovery ranges.

Configuring SNMP Services on Windows

1. Open a command run prompt and type **services.msc** to open the Services MMC.
2. Right-click **SNMP Service**, and select **Properties**. If you cannot locate SNMP Service, you must install it using **Add/Remove Windows Components**.
3. Click **Security** and ensure that **Accept SNMP packets from any host** is selected.
4. Under **Accepted Community Names**, ensure that **public** (or a customized community string) is set. If not set by default, click **Add**, and type a community string in **Community Name**. Also select community rights as **READ ONLY** or **READ WRITE**.
5. Click **Traps** and ensure that the community string field has a valid name.
6. In **Trap destination**, click **Add** and enter the Open Manage Essential Console IP address.
7. Start the service.

Configuring SNMP Services on Linux

1. Run the command `rpm -qa | grep snmp`, and ensure that the **net-snmp** package is installed.
2. Run `cd /etc/snmp` to navigate to the snmp directory.
3. Open **snmpd.conf** in the VI editor (**vi snmpd.conf**).
4. Search snmpd.conf for **# group context sec.model sec.level prefix read write notif** and ensure that the values for fields read, write, and notif are set to **all**.
5. At the end of the **snmpd.conf** file, just before Further Information, enter the Open Manage Essentials Console IP address in the following format: `trapsink <OPEN MANAGE ESSENTIALS CONSOLE IP> <community string>` For example, `trapsink 10.94.174.190 public`.
6. Start the SNMP services (service snmpd restart).

Troubleshooting Receiving SNMP Traps

If you encounter a problem receiving SNMP traps, perform the following steps to troubleshoot and fix the problem:

1. Check for network connectivity between the two systems. You can do this by pinging one system from another using the ping <IP address> command.
2. Check the SNMP configuration on the managed node. Ensure that you have specified the OpenManage Essential console IP address and the community string name in the SNMP services of the managed node.
For information on setting SNMP on a Windows system, see [Configuring SNMP Services on Windows](#).
For information on setting SNMP on a Linux system, see [Configuring SNMP Services on Linux](#).

3. Ensure that the SNMP Trap service services are running in the Open Manage Essentials system.
4. Check firewall settings to allow UDP 161, 162 ports.

Troubleshooting Discovery of Windows Server 2008–Based Servers

You also have to allow the server discovery. By default, the option is disabled in Windows Server 2008.

1. Click **Start** → **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Advanced Sharing Setting**.
2. Choose the drop-down arrow for the applicable network profile (Home or Work / Public) and under **Network Discovery**, select **Turn on network discovery**.

Troubleshooting SNMP Traps for ESX or ESXi Versions 3.5, 4.x, or 5.0

Details: To generate virtual machine and environmental traps from ESX or ESXi 3.5 or 4.x hosts, configure and enable the embedded SNMP agent. You cannot use the Net-SNMP-based agent to generate these traps, although it can receive GET transactions and generate other types of traps.

This represents a change in behavior from ESX 3.0.x, in which the configuration file for the Net-SNMP-based agent controlled the generation of virtual machine traps

Solution: Use the `vicfg-snmp` command from the Remote CLI or vSphere CLI to enable the SNMP agent and configure trap destinations. Each time you specify a target with the `vicfg-snmp` command, the settings you specify overwrite all previously specified settings. To specify multiple targets, specify them in a single command, separated by commas.

Troubleshooting Problems With Microsoft Internet Explorer

Follow the instructions in this section if you are experiencing any of the following:

- Unable to open OpenManage Essentials using Internet Explorer.
- Internet Explorer displays certificate errors.
- Internet Explorer displays a message to approve the certificate.
- Unable to browse the file system to deploy Server Administrator and system update.
- Unable to display the Device tree for devices.
- Unable to install active components.

1. Open OpenManage Essentials on the client server using Internet Explorer.
2. Click **Tools** → **Internet Options** → **Security**.
3. Select **Local intranet** and click **Sites**.
4. Click **Advanced**.
5. Type the fully qualified name of the server where OpenManage Essentials is installed.
6. Click **Add**.

If the issue persists, there may be an issue with the DNS server resolving the name of the OpenManage Essentials server. See [Resolving DNS Server Issues](#).

If a certificate error is displayed:

- Contact your system administrator to add the OpenManage Essentials certificate published to the 'Trusted Root Certificate Authorities' and Trusted Publishers' on domain systems.
- Add the OpenManage Essentials certificate to your 'Trusted Root Certificate Authorities' and 'Trusted Publishers' certificate stores using Internet Explorer.

Resolving DNS Server Issues

To resolve DNS server issues:

1. Contact your system administrator and add the name of the system running OpenManage Essentials to the DNS server.
2. Edit your host file to resolve the IP of the system running OpenManage Essentials. The host file is located at `%windir%\System32\drivers\etc\hosts`.
3. Add the IP of the system running OpenManage Essentials to the Local intranet sites in Internet Explorer.



NOTE: You cannot remove the certificate errors unless you use the fully qualified name of the server running OpenManage Essentials.

Troubleshooting Map View

Question: Why is the **Map View** feature not available?

Answer: The **Map View** feature is available only if you have discovered any PowerEdge VRTX CMC or PowerEdge FX2/FX2s devices with an Enterprise license, using the WS-Man protocol. If the device with an Enterprise license is discovered using the SNMP protocol, the **Map View** feature is not available. Rediscovering the device using the WS-Man protocol is required, if the **Map View** tab is not displayed in the device details portal for a licensed device.

Question: Why am I unable to add a particular device on the map?

Answer: Only PowerEdge VRTX and PowerEdge FX2/FX2s devices with an Enterprise license can be added to the map.

Question: The map does not load with the MapQuest or Bing map provider. What should I do?

Answer: This indicates a problem with the Internet connectivity.

- Verify if you are able to connect to the Internet through the browser.
- If the system connects to the Internet through the proxy:
 - For MapQuest map provider — Configure the proxy settings in the OpenManage Essentials **Settings** → **General Settings** page.
 - For Bing map provider — Verify if you configured the proxy server settings in Internet Explorer.
- Verify if you are able to access the MapQuest website.

Question: Why is the map loading slowly?

Answer: The map may load slowly as it requires more network bandwidth and graphic processing capability compared to normal browsing. Constant zooming and panning on the map may also slow the loading of the map.

Question: Why I am unable to locate an address using the search bar or **Edit Device Locations** dialog box?

Answer: There may be a problem with your Internet connection or the map provider may not be able to resolve the address.

- Verify if the valid map provider key is entered in the **Map Settings**.
- Verify if you are able to connect to the Internet through the browser.
- If the system connects to the Internet through the proxy:
 - For MapQuest map provider — Configure the proxy settings in the OpenManage Essentials **Settings** → **General Settings** page.
 - For Bing map provider — Verify if you configured the proxy server settings in Internet Explorer.
- Try to provide a variation of the address you provided. You can try providing a complete address. Abbreviations such as state, country, airport code, may have an unexpected result.

Question: Why cannot I use one map provider on the **Home** portal and another on the **Devices** portal?

Answer: The **Map View** available through the **Home** portal and the **Devices** portal are synchronized. Changes to the **Settings** or device locations on the **Map View** are affected on both the portals.

Question: How can I enhance the **Map View** experience?

Answer: Improving the network bandwidth accelerates the loading of the map. A more powerful graphic card enables faster zooming and panning capability. When using the MapQuest provider, the map is rendered better if OpenManage Essentials is launched on the management server.

Frequently Asked Questions

Installation

Question: How do I install OpenManage Essentials using a remote SQL database named instance?

Answer: To connect remotely, the SQL Server with named instances requires a running **SQL Server Browser** service.

Question: Will OpenManage Essentials support Microsoft SQL Server Evaluation edition?

Answer: No, SQL Server Evaluation edition is not supported.

Question: What are the minimum login roles for SQL Server?

Answer: See [Minimum Login Roles for Microsoft SQL Server](#) and [Terms and Conditions for Using Relational Database Management Systems](#).

Question: When launching the OpenManage Essentials installer, an error message is displayed, stating a failure to load a specific library (for example, `failed to load OMIL32.DLL`), a denial of access, or an initialization error. What do I do?

Answer: This issue is most likely due to insufficient Component Object Model (COM) permissions on the system. To remedy this situation, see support.installshield.com/kb/view.asp?articleid=Q104986. The OpenManage Essentials installer may also fail if a previous installation of systems management software or some other software product was unsuccessful. Delete the following temporary windows installer registry, if present: `HKLM\Software\Microsoft\Windows\CurrentVersion\Installer\InProgress`.

Question: During the installation of Microsoft ASP .NET prerequisite, I am getting the following error message: **One of the prerequisites has failed to install. The one click prerequisite installer will now exit.** What do I do?

Answer: To resolve this issue, perform one of the following:

- Run the Windows update and ensure all the updates are installed successfully.
- Download and install the required security certificates. For more information on the required security certificates, see <https://blogs.msdn.microsoft.com/vsnetsetup/2016/03/28/a-certificate-chain-could-not-be-built-to-a-trusted-root-authority-2/>.

Upgrade

Question: What troubleshooting can I do for the following error message:

`Https error 503. The service is unavailable?`

Answer: To resolve this issue, perform an IIS reset and launch OpenManage Essentials. To perform an IIS reset, launch the command prompt and type `iisreset`. When an `iisreset` is done, all connections to the web server are reset. It also resets any website hosted on the same OpenManage Essentials server.

Question: Why does an upgrade to the latest version of OpenManage Essentials fail in a large deployment scenario?

Answer: To resolve this issue, ensure that the system meets the minimum hardware requirements. For more information, see the **Minimum Recommended Hardware** section in the *Dell EMC OpenManage Essentials User's Guide* at Dell.com/OpenManageManuals.


Question: How do I upgrade to OpenManage Essentials version 2.1, when OpenManage Essentials version 1.1 is installed on a remote database with SQL Server 2005?

Answer: Installation or upgrade of OpenManage Essentials version 2.1 is not supported on Microsoft SQL Server 2005 (all editions) either on a local or remote database. While upgrading from OpenManage Essentials version 1.1 installed with remote SQL Server 2005 to OpenManage Essentials version 2.1, the following message is displayed:

Dell EMC OpenManage Essentials cannot be installed or upgraded on SQL Server versions prior to SQL Server 2008. Refer to the FAQ for information on possible migration and additional details.

In this case, you can manually migrate the data from SQL Server 2005 and then upgrade to OpenManage Essentials version 2.1 as follows:

1. Create a backup of the OpenManage Essentials version 1.1 database.
2. Migrate the OpenManage Essentials version 1.1 data from SQL Server 2005 to SQL Server 2008, 2008 R2, or 2012. For more information, see the *OpenManage Essentials Database re-target process* instructions at <https://en.community.dell.com/techcenter/systems-management/f/4494/t/19440364.aspx>.
3. Ensure that OpenManage Essentials version 1.1 can connect to migrated database and works as expected.
4. Launch the OpenManage Essentials version 2.1 installer to complete the upgrade.

 **NOTE:** After upgrading to OpenManage Essentials version 2.1 with SQL Server 2012, the SQLEXPRESSOME instance is created and data from OpenManage Essentials version 1.1 is migrated to OpenManage Essentials Version 2.1.

Question: After upgrading from OpenManage Essentials version 2.2 to version 2.5, duplication of the PowerVault MD Series storage arrays is observed in the device tree. What should I do?

Answer: To eliminate the duplicate entries, ensure that you delete and rediscover the PowerVault MD Series storage arrays.

Question: Can I upgrade the server operating system with OpenManage Essentials installed?

Answer: It is not recommended to upgrade the server operating system with OpenManage Essentials installed. If you continue with the upgrade, then OpenManage Essentials will not work as expected. To upgrade the operating system, perform the following steps:

1. Create a backup of the OpenManage Essentials database.
2. Uninstall OpenManage Essentials. For more information, see [Uninstalling OpenManage Essentials](#)
3. Upgrade the server operating system.
4. Reinstall OpenManage Essentials and select the previously backed up database during the installation.

Tasks

Question: What troubleshooting can I do if a software update task or remote task fails to create or run?

Answer: Ensure that the DSM Essentials Task Manager service is running in Windows services.

Question: When accessing OpenManage Essentials from a remote system, is it possible to create a remote task to deploy OMSA/iDRAC Service Module on a target device using an OMSA/iDRAC Service Module package that is available on that particular remote system?

Answer: No. The remote task to deploy OMSA/iDRAC Service Module on a target device should be created by accessing OpenManage Essentials from the server where OpenManage Essentials is installed/running.

Question: How do I use command line features while deploying OpenManage Server Administrator?

Answer: Unattended installation provides the following features:

- A set of optional command line settings to customize an unattended installation.
- Customization parameters to designate specific software features for installation.

Question: The 'chassis power on' IPMI command line task is unsuccessful. The following error is displayed: **Unable to establish IPMI v2/ RMCP+ session, Unable to set Chassis Power Control to Up/On**. What can I do to resolve the error?

Answer: The error may occur if the iDRAC has either an issue or several tasks in queue. Try resetting the iDRAC and run the task again.

Optional Command Line Settings

The following table shows the optional settings available for the **msiexec.exe** MSI installer. Type the optional settings on the command line after **msiexec.exe** with a space between each setting.

 **NOTE:** See support.microsoft.com for full details about all the command line switches for the Windows Installer Tool.

Table 258. Command Line Settings for MSI Installer

Setting	Result
/i <Package Product Code>	This command installs or configures a product.

Setting	Result
	/i SysMgmt.msi – Installs the Server Administrator software.
/i SysMgmt.msi /qn	This command carries out a fresh installation of version 6.1.
/x <Package Product Code>	This command uninstalls a product. /x SysMgmt.msi – Uninstalls the Server Administrator software.
/q[n b r f]	This command sets the user interface (UI) level. /q or /qn – no UI. This option is used for silent and unattended installation. /qb – basic UI. This option is used for unattended but not silent installation. /qr – reduced UI. This option is used for unattended installation while displaying a modal dialog box showing install progress. /qf – full UI. This option is used for standard attended installation.
/f[p o e d c a u m s v]<Package ProductCode>	This command repairs a product. /fp – This option reinstalls a product only if a file is missing. /fo – This option reinstalls a product if a file is missing or if an older version of a file is installed. /fe – This option reinstalls a product if a file is missing or an equal or older version of a file is installed. /fd – This option reinstalls a product if a file is missing or a different version of a file is installed. /fc – This option reinstalls a product if a file is missing or the stored checksum value does not match the calculated value. /fa – This option forces all files to reinstall. /fu – This option rewrites all required user-specific registry entries. /fm – This option rewrites all required system-specific registry entries. /fs – This option overwrites all existing shortcuts. /fv – This option runs from the source and re-caches the local package. Do not use the /fv reinstall option for the first installation of an application or feature.
INSTALLDIR=<path>	This command installs a product to a specific location. If you specify an install directory with this switch, it must be created manually prior to executing the CLI install commands or they fail with no error or message. /i SysMgmt.msi INSTALLDIR=c:\OpenManage /qn – installs a product to a specific location using c:\OpenManage as the install location.

For example, running **msiexec.exe /i SysMgmt.msi /qn** installs Server Administrator features on each remote system based on the system's hardware configuration. This installation is done silently and unattended.

Customization Parameters

REINSTALL and **REMOVE** customization CLI parameters provide a way to customize the exact software features to install, reinstall, or uninstall when running silently or unattended. With the customization parameters, you can selectively install, reinstall, or uninstall software features for different systems using the same unattended installation package. For example, you can choose to install Server Administrator, but not Remote Access Controller service on a specific group of servers, and choose to install Server Administrator, but not Storage Management Service, on another group of servers. You can also choose to uninstall one or multiple features on a specific group of servers.

 **NOTE: Type the REINSTALL, and REMOVE CLI parameters in upper case, as they are case-sensitive.**

 **NOTE: The software feature IDs mentioned in the following table are case-sensitive.**

Table 259. Software Feature IDs

Feature ID	Description
ALL	All features
BRCM	Broadcom NIC Agent
INTEL	Intel NIC Agent
IWS	OpenManage Server Administrator Web Server
OMSM	Server Administrator Storage Management Service
RmtMgmt	Remote Enablement
RAC4	Remote Access Controller (DRAC 4)
RAC5	Remote Access Controller (DRAC 5)
iDRAC	Integrated Dell Remote Access Controller
SA	Server Administrator

 **NOTE: Only iDRAC6 is supported on xx1x systems.**

You can include the **REINSTALL** customization parameter on the command line and assign the feature ID (or IDs) of the software feature that you would like to reinstall. An example is:

```
msiexec.exe /i SysMgmt.msi REINSTALL=BRCM /qb.
```

This command runs the installation for OpenManage Systems Management and reinstall only the Broadcom agent, in an unattended but not silent mode.

You can include the **REMOVE** customization parameter on the command line and assign the feature ID (or IDs) of the software feature that you would like to uninstall. For example:


```
msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qb.
```

This command runs the installation for OpenManage Systems Management and uninstalls only the Broadcom agent, in an unattended but not silent mode.

You can also choose to install, reinstall, and uninstall features with one execution of the **msiexec.exe** program. For example:

```
msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qb
```

This command runs the installation for managed system software, and uninstalls the Broadcom agent. This execution is in an unattended but not silent mode.

 **NOTE: A Globally Unique Identifier (GUID) is 128 bits long, and the algorithm used to generate a GUID guarantees each GUID to be unique. The product GUID uniquely identifies the application. In this case, the product GUID for Server Administrator is {54C04D53-C3C3-46EA-A75F-7AFF4BEB727C}.**

MSI Return Code

An application event log entry is recorded in the **SysMgmt.log** file. Table 3 shows some of the error codes returned by the **msiexec.exe** Windows Installer Engine.

Table 260. Windows Installer Return Codes

Error Code	Value	Description
ERROR_SUCCESS	0	The action is completed successfully.
ERROR_INVALID_PARAMETER	87	One of the parameters was invalid.
ERROR_INSTALL_USEREXIT	1602	The user canceled the installation.

Error Code	Value	Description
ERROR_SUCCESS_REBOOT_REQUIRED	3010	A restart is required to complete the installation. This message is indicative of a successful installation.

 **NOTE:** See support.microsoft.com for full details on all the error codes returned by the `msiexec.exe` and `InstMsi.exe` Windows installer functions.

E-mail Alert Action

Question: Why am I not receiving e-mails after setting up e-mail alert action?

Answer: If you have an Antivirus Client installed on the system, then configure it to allow e-mails.

Discovery

Question: Why are SUSE Linux Enterprise and Red Hat Enterprise Linux based-servers not displayed in the **Server** category after I have discovered it using SSH protocol?

Answer: The OpenManage Essentials SSH plugin uses `sshlib2`. `sshlib2` fails to authenticate Linux servers which have disabled the **Authentication by password** option. To enable the option:

1. Open the file `/etc/ssh/sshd_config` in edit mode and search for the key **PasswordAuthentication**.
2. Set the value to yes, and save the file.
3. Restart the sshd service `/etc/init.d/sshd restart`.

The servers are now displayed under the **Server** category in the **Device** tree.

Question: What troubleshooting can I do if a discovery task fails to create or run?

Answer: Ensure that the DSM Essentials Task Manager service is running in Windows services.

Question: Why are my ESX virtual machines not correlated with their ESX host server?

Answer: You must discover the ESXi host server using SNMP and WSMAN or the guest virtual machine will not correlate correctly when discovered using SNMP.

Question: Why are devices discovered with WMI getting classified as Unknown?

Answer: WMI discovery classifies a device as unknown when the credential for a user account in the Administrators group (not Administrator) is supplied for the discovery range in some cases.

If you are seeing this issue, read the KB article at support.microsoft.com/?scid=kb;en-us;951016 and apply the registry work as described. This resolution applies to managed nodes with Windows Server 2008 R2.

Question: Why are Dell devices discovered using WS-Man with root CA certificate getting classified as Unknown?

Answer: There may be a problem with the root certificate you are using to discover the WS-Man target(s). For instructions to discover and inventory WS-Man target(s) using a root CA certificate, see [Discovering and Inventorying Dell Devices Using WS-Man Protocol With a Root Certificate](#).

Question: What are SNMP authentication traps?

Answer: An authentication trap is sent when an SNMP agent is hit with an enquiry that contains a community name it does not recognize. The community names are case-sensitive.

The traps are useful to find if someone is probing a system, although its better nowadays to just sniff packets and find out the community name.

If you use multiple community names on the network, and some management might overlap, users may want to turn these off as they become false positives (annoyances).

For more information, see technet.microsoft.com/en-us/library/cc959663.aspx.

When an SNMP agent receives a request that does not contain a valid community name or the host that is sending the message is not on the list of acceptable hosts, the agent can send an authentication trap message to one or more trap destinations (management systems). The trap message indicates that the SNMP request failed authentication. This is a default setting.

Question: Why does OpenManage Essentials not support entering host names with underscore in the discovery wizard?

Answer: Per RFC 952, underscores are not valid in DNS names. A *name* (net, host, gateway, or domain name) is a text string up to 24 characters drawn from the alphabet (A-Z), digits (0-9), minus sign (-), and period (.). Periods are only allowed when they serve to delimit components of domain style names.

For more information see ietf.org/rfc/rfc952.txt and zytrax.com/books/dns/apa/names.html.

Question: What is On-demand?

Answer: On-demand is an operation where a managed system is checked for status/health by OpenManage Essentials when an SNMP trap is received. There are no settings to be changed to enable the on-demand feature. However, the IP address of the management system must be available in the trap destination of SNMP service. An SNMP trap is received from the managed system when there is an issue or failure of a server component. These traps can be viewed under the alert logs.

Question: I have discovered the server with the SNMP protocol, but the RAC name of the iDRAC is not displayed in the device tree, portals, and wizards.

Answer: RAC name is displayed only if you have discovered the iDRAC with the WS-Man protocol. Otherwise, the system name is displayed instead of the RAC name.

Question: Why do devices that are already discovered disappear from the device tree during discovery?

Answer: This issue occurs when there are duplicate MAC addresses, which are typically observed with virtual devices that may have MAC addresses that contain only 16 zeroes.

To resolve this issue:

1. Ensure that you are logged in to the operating system with administrative privileges.



NOTE: Ensure that you create a backup copy of the `dconfig.ini` file before you make any changes.

2. Open the `dconfig.ini` file available at `SysMgt\Essentials\configuration`.
3. Edit the `PRIVATE_MAC_EXCLUDE_LIST` line as follows:
`PRIVATE_MAC_EXCLUDE_LIST=127.0.0.1,0.0.0.0,005345000000,33506F453030,505054503030,0000FFFFFFFF,204153594EFF,000000000000,00000000000000e0,020054554e01,204153594eff,0000000000000000`
4. Save the `dconfig.ini` file, and restart the **OpenManage Essentials** services.

Question: I discovered a PowerEdge FN IO Aggregator (IOA) with SNMP protocol. Why is the Service Tag of the FN IOA displayed as N/A in the device inventory?

Answer: FN IOAs that were manufactured prior to February 1, 2016 do not have a Service Tag. Therefore, the Service Tag is displayed as N/A.

Question: When trying to discover the Dell devices using WS-Man protocol, an error message is displayed, stating a failure to connect with basic authentication. What do I do?

Answer: This issue is because, the authentication type **Basic** was not enabled on the OpenManage Essentials system. To enable the **Basic** authentication type on OpenManage Essentials system, see the **Authentication for Remote Connections** knowledge base article at Microsoft.com.

Below is the expected configuration for winrm to work:

```
>winrm get winrm/config/client
```

```
Client
```

```
NetworkDelaysms = 5000
```

```
URLPrefix = wsman
```

```
AllowUnencrypted = false
```

```
Auth
```

```
Basic = true
```

```
Digest = true
```

```
Kerberos = true
```

```
Negotiate = true
```

```
Certificate = true
```

```
CredSSP = false
```

```
DefaultPorts
```

```
HTTP = 5985
```

HTTPS = 5986

TrustedHosts

Question: I have discovered a PowerEdge R830 server by using in-band method. OMSA version 8.3 is also installed on the server. Why am I unable to view the software inventory information of the iDRAC and network cards such as Mellanox, QLogic, and Intel?

Answer: To get the software inventory information of the network cards, you must either discover the PowerEdge R830 server by using out-of-band method or run the Firmware and Driver Inventory task for the server.

Question: Why is OpenManage Essentials unable to run discovery, inventory or status polling tasks for iDRACs or CMCs with the WS-Man protocol?

Answer:

1. Open the Troubleshooting Tool, and run the WS-Man test for the target devices.
2. If the test results specify that TLS 1.1 or 1.2 is enabled on the device, perform the following steps on the system where OpenManage Essentials is installed:
 - a. Install the update available in KB3140245 at Microsoft.com to enable TLS protocols in winrm.
 - b. Set the default protocol as TLS 1.2 with a DWORD registry entry `DefaultSecureProtocols` in:
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp`
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp`
 - Set the value to **0x0000A00** for enabling TLS 1.0, 1.1 and 1.2.
 - c. Restart the system, and then retry the tasks in OpenManage Essentials.

Question: Why do the create template or apply template tasks fail for CMC?

Answer:

1. Open the Troubleshooting Tool, and run the WS-Man test for the target devices.
2. If the test results specify that TLS 1.1 or 1.2 is enabled on the device, perform the following steps on the system where OpenManage Essentials is installed:
 - a. To enable TLS in the web browser:
 1. Click **Start** → **Run**, type `inetcpl.cpl` and press Enter.
 2. Click the **Advanced** tab.
 3. In the **Security** section, select **Use TLS 1.0**, **Use TLS 1.1**, and **Use TLS 1.2**.
 - b. To enable TLS for all user accounts:
 1. Create a DWORD registry entry `SecureProtocols` in `[HKLM]\Software\Microsoft\Windows\CurrentVersion\Internet Settings`.
 2. Set the value to **0xA80** to enable support for TLS 1.0, TLS 1.1, and TLS 1.2.
 - c. Restart the system, and then retry the tasks in OpenManage Essentials.

Question: Why does the RACADM Command Line task fail on iDRACs or CMCs?

Answer:

1. Open the Troubleshooting Tool, and run the WS-Man test for the target devices.
2. If the test results specify that TLS 1.1 or 1.2 is enabled on the device, perform the following steps on the system where OpenManage Essentials is installed:
 - a. To enable TLS in the web browser:
 1. Click **Start** → **Run**, type `inetcpl.cpl` and press Enter.
 2. Click the **Advanced** tab.

3. In the **Security** section, select **Use TLS 1.0**, **Use TLS 1.1**, and **Use TLS 1.2**.
- b. To enable TLS for all user accounts:
 1. Create a DWORD registry entry `SecureProtocols` in `[HKLM]\Software\Microsoft\Windows\CurrentVersion\Internet Settings`.
 2. Set the value to **0xA80** to enable support for TLS 1.0, TLS 1.1, and TLS 1.2.
- c. Restart the system, and then retry the tasks in OpenManage Essentials.

Question: After discovering two Fibre Channel switches that have the same device name and the Service Tag as none, only one switch is displayed in the device tree. What should I do to ensure that both devices are displayed in the device tree?

Answer: Assign a unique name to both the switches and discover them again.

Inventory

Question: What troubleshooting can I do if an inventory task fails to create or run?

Answer: Ensure that DSM Essentials Task Manager service is running in Windows services.

Question: The Software Inventory Information table displays multiple entries of "Base System Device Driver" after the Firmware & Driver Inventory collection task or Discovery/Inventory. What should I do?

Answer: To resolve the issue, verify if the chipset driver is installed on the server. If the chipset driver is not installed, install the latest chipset driver and then reboot the server. After rebooting the server, rediscover the server in OpenManage Essentials.

Question: I discovered a PowerEdge FX or FX2s chassis with firmware version 1.1 using the WS-Man protocol. The device is not displayed in the **System Update** → **Non-Compliant Systems** tab. However, the Software Inventory table is not displayed. What should I do?

Answer: Manually (outside of OpenManage Essentials) upgrade the PowerEdge FX or FX2s firmware to version 1.2 or later.

Question: An ESXi server is displayed under the **System Update** → **Non-Inventoried Systems** tab. I ran the inventory task from the **Non-Inventoried Systems** tab, however, the device is still displayed under the **Non-Inventoried Systems** tab.

Answer: Inventory information of an ESXi server may not be retrieved if the host name of the server cannot be resolved to its IP address. To resolve the issue:

1. Ping the host name of the server and verify the resulting IP address.
2. If the IP address is not the same as the IP address of the ESXi server, configure the IP address of the ESXi server correctly in the DNS server.
3. Run the inventory again.

Question: A modular server with iDRAC6 discovered using WS-Man protocol with the default WS-Man Timeout and Retries values is classified under the **RAC** device group. However, no inventory information is displayed. What should I do?

Answer: Verify the WS-Man Timeout setting used for discovery and ensure that the timeout value is within the 4 to 99 range.

Question: I discovered a few blade servers hosted within a chassis using the SNMP protocol. Later, I discovered the Dell chassis and its components using the **Chassis (CMC) Discovery – All Components** filter of the **Guided Wizard**. I notice that the discovery range group of the previously discovered blade servers has moved within the discovery range group of the chassis. However, the blade servers that I had discovered earlier are still inventoried using the SNMP protocol. What should I do?

Answer: It is recommended that you either discover each blade server individually or discover the chassis and its components using the **Chassis (CMC) Discovery – All Components** filter of the **Guided Wizard**. If you had discovered a few blade servers prior to discovering the chassis using the **Chassis (CMC) Discovery – All Components** filter of the **Guided Wizard**, perform the following:

1. Edit the chassis discovery range group.
2. Select the **Chassis (CMC) Discovery – All Components** filter.
3. Provide the credentials of the chassis and the blade servers (iDRACs).



NOTE: Provide the iDRAC credentials only if the iDRAC credentials are not the same as the chassis credentials.

4. Save the changes.
5. Right-click the chassis range group and click **Perform Discovery and Inventory Now**.

The blade servers will use the WS-Man credentials during the next inventory cycle.

System Update

Question: As an OpenManage Essentials administrator (OMEAdmin), what do I do if I am unable to perform system updates on devices?

Answer: To resolve this issue, perform one of the following steps:

- Add the OMEAdmin to the server administrator group.
- Reduce the user control settings by clicking **Start** → **Control Panel** → **User Accounts** → **Change User Account Control Settings**.

Question: What do I do if iDRAC does not download packages?

Answer: To resolve this issue, ensure that:

- The default website is enabled in IIS.
- The virtual folder (**install_packages**) is present and is pointing to the **SystemUpdate** folder.

The default website is enabled in IIS.

Question: What order are packages installed on a system?

Answer: Packages are applied in the following order:

1. Driver
2. Firmware
3. Firmware ES
4. BIOS

Question: How do I configure Internet Explorer with Enhanced Security Configuration to ensure that OpenManage Essentials can utilize all features that use resources from Dell online?

Answer: To ensure that these features work in the Open Manage Essentials console on an environment with Internet Explorer Enhanced Security Configuration enabled. The user needs to add ***.dell.com** to the **Trusted sites** zone.

Import Catalog and *System Update* require internet access when the user selects Dell Online as the source.

The warranty report also uses Dell online resources to retrieve information and also will not return data without it.

Question: What if IPMI is disabled after installing BMC Utility?

Answer: Try restarting DSM Essentials Network Monitor Service, DSM Essentials Task Manager service, and restart IIS.

Question: What is Omremote?

Answer: Omremote enables you to execute remote Server Administrator command line tasks (inband) and also helps you to deploy Server Administrator on remote Dell servers. Omremote is an executable file that is located at C:\Program Files\Dell\SystMgt\Essentials\bin folder. It uses WMI connection for the Windows-based devices and SSH for the Linux-based devices. Ensure that the required ports are opened. Omremote commands require a Server Administrator supported operating system with the Server administrator installed. To install/update Server administrator on the remote system, you must use an operating system preinstall package.

Question: A system update task for applying a firmware update on a hard drive that is inaccessible or degraded results in an error. What can I do?

Answer: Follow the troubleshooting instructions in the "Physical Disk Failures and Rebuilds" section of the [How to troubleshoot hard drive and RAID controller errors on Dell PowerEdge 12G servers](#) Dell Knowledge Base article, and then retry the system update task.

Question: When I applied an applicable Dell Update Package (DUP) on a device running a 32-bit Linux operating system, the following message is displayed: **This package does not support running on 32-bit operating systems**. What could be the reason?

Answer: DUPs for Linux may include packages that are applicable for both 64-bit and 32-bit operating systems. OpenManage Essentials displays both 64-bit and 32-bit packages as applicable packages, irrespective of the operating system of the target device. Therefore, you may notice the message while applying 64-bit Linux update packages on devices running 32-bit Linux operating systems.

Question: How do I load a Dell catalog for software update? Or What do I do when I get errors when trying to run software update tasks?

Answer:

1. Download the catalog to the OpenManage Essentials system directly or use a System Update Utility DVD in the local system drive.
2. Browse for **catalog.xml** file on the local system or DVD (not on a file share, it is possible to use a file share, but for troubleshooting, do not use file share).
3. Now, create software update tasks. If tasks fail, more information is found in the task details.
4. Try setting all internet explorer security settings to LOW if tasks do not run.

Managing Device Configurations

Question: Why are unsupported device groups shown in the Device Configuration wizard?

Answer: All user created visible custom groups are shown in the device selection screen. A custom group may contain invalid system groups for the given wizard. The invalid system groups can be ignored.

Question: If I filter the attributes and then save the device configuration template, will the template include only the filtered attributes?

Answer: No, the template will include all the attributes. Filtering the attributes does not have any effect on the attributes that are saved. To remove the attributes from a template, clear the Deploy check boxes for the attributes, and then save the template.

Question: Why is a device that is already associate to the current template displayed in the device selection page?

Answer: The device selection page displays the all applicable devices including the device that is currently associated with the template. You can ignore the currently associated device and select another device, if required.

Question: Why does the **Data Sources** table in the device inventory displays additional or duplicate information with an **Unknown** health status for the same agent?

Answer: This issue may occur in the following scenarios:

- The Data Source information of the agent is no longer in use while connecting to OpenManage Essentials.
- The agent is unable to determine the health and connection status of the device.
- The agent is unreachable or unresponsive.

To resolve this issue, delete the device and discover the device again.

Device Group Permissions

Device Group Permissions Portal

Question: Can I add a user group to the **OmeSiteAdministrators** role?

Answer: Yes, you can add a user group to the **OmeSiteAdministrators** role.

Question: Can I add an OmeAdministrator to the **OmeSiteAdministrators** role?

Answer: Yes, you can add an OmeAdministrator to the **OmeSiteAdministrators** role. The user will have all the rights of the OmeAdministrator. However, to effectively manage device group permissions, it is recommended that a member of the OmeSiteAdministrators role is removed from the OmeAdministrators and OmePowerUsers roles.

Question: Can I add a user who has not logged on to OpenManage Essentials to the **OmeSiteAdministrators** role?

Answer: Yes, you can use the **Edit Members of OmeSiteAdministrators** wizard to add a user who has not logged on to OpenManage Essentials to the **OmeSiteAdministrators** role.

Question: What happens if a OmePowerUser is added to the **OmeSiteAdministrators** role?

Answer: Roles and permissions are additive. The user will not have all of (but retain some of) the restrictions of a OmeSiteAdministrator. The user will be able to perform edit actions that the OmeSiteAdministrator was not able to perform. Target security cannot be guaranteed for this type of user (they can edit device groups assigned to them).

Question: Can I promote an OmeSiteAdministrator to an OmeAdministrator?

Answer: Yes, the user will have all rights and will be able to target all devices. It is suggested, but not required, to remove the user from the **OmeSiteAdministrators** role before adding the user to the **OmeAdministrators** role.

Question: How do I add a current OmeAdministrator to the **OmeSiteAdministrators** role?

Answer:

1. Remove the user from the **OmeAdministrators** Windows user group.
2. In the **Device Group Permissions** portal, use the **Edit Members of OmeSiteAdministrators** option to select and add the user to the **OmeSiteAdministrators** role.
3. When the user logs in again, the user will be an OmeSiteAdministrator.

Question: A user is removed from the **OmeAdministrators** role and then added to the **OmeSiteAdministrators** role. What happens to the tasks that were created while the user was an OmeAdministrator?

Answer: The task created when the user was an OmeAdministrator can still be executed on the targets selected at the time of task creation.

Remote and System Update Tasks

Question: What happens to the task target for a remote task if the **OmeSiteAdministrators** device group permissions change?

Answer: The task targets of a remote task are not affected by changes to device group permissions. Remote tasks that were created earlier may have task targets that the OmeSiteAdministrator is not assigned to.

Question: What must an OmeSiteAdministrator do to edit a task?

Answer: If the OmeSiteAdministrator is the owner of the task, the OmeSiteAdministrator must delete the existing task and create a new task.

Question: Can an OmeSiteAdministrator re-run a task?

Answer: Yes, A task can be re-run if the task was created earlier by the OmeSiteAdministrator.

Question: Can an OmeSiteAdministrator re-run a task after the user name of the OmeSiteAdministrator is changed?

Answer: No, the OmeSiteAdministrator must re-create the tasks if the user name is changed.

Question: Can two **OmeSiteAdministrators** assigned to the same custom device group, use the tasks created by each other?

Answer: No, the **OmeSiteAdministrators** can only use the tasks they have created.

Custom Device Groups

Question: Can an OmeSiteAdministrator delete devices in any group?

Answer: Yes, the OmeSiteAdministrator can delete devices in any group, similar to the OmePowerUser or OmeAdministrator.

Question: Can **OmeSiteAdministrators** edit the device groups they created?

Answer: No, the **OmeSiteAdministrators** cannot edit device groups or queries.

Question: Can **OmeSiteAdministrators** delete queries and custom groups?

Answer: Yes, the **OmeSiteAdministrators** can delete queries and custom groups.

Question: Can **OmeSiteAdministrators** add devices to a custom device group?

Answer: No, the **OmeSiteAdministrators** cannot edit a custom device group.

Deployment and Configuration Compliance

Question: Can an OmeSiteAdministrator perform the right-click actions available on device configuration templates in the **Deployment** and **Device Compliance** portals?

Answer: Yes, the OmeSiteAdministrator can perform all right-click actions available on device configuration templates in the **Deployment** and **Device Compliance** portals.

Deployment and Configuration Compliance

Question: What is FQDD?

Answer: A Fully Qualified Device Descriptor (FQDD) is used to identify a specific component in a system. Typically, a device configuration template contains FQDDs for the various components of a system and their corresponding setting values. For example, the FQDD for the iDRAC may be represented as iDRAC.embedded.1. For components such as the network cards (NICs) that have more than one port or partition, the FQDD may be represented as:

- NIC.Integrated.1-2-2, which represents partition 2 of port 2 of a NIC that is integrated on the system board.
- NIC.Slot-3.1.2, which represents partition 2 of port 1 that is available on a NIC adapter that is inserted in slot 3 on the system board.

Question: After a deployment task is completed, the results section on the task **Execution Details** window displays the same FQDD for all partitions of a NIC. How do I verify if the correct values are deployed?

Answer: In some cases, when attribute values are deployed to multiple partitions, the FQDD values shown in the results tab may be incorrect (specifically, the same FQDD may be repeated for different partitions). However, correct values are stored in the database. You can view the device configuration inventory to see the actual values.

Question: I replaced a server (source) with another server (target) from a compute pool. Will the existing alerts and tasks be associated to the target server?

Answer: The following are the expected behaviors after replacing the server (where source refers to the source operating system):

- Alerts and tasks that were created before replacing the server are associated only with source server.
- Alerts and tasks that are created after the replacing the server are associated only with the target server.

Question: When OpenManage Essentials performs deployment in QLogic CNA cards, sometimes the value of second octet for virtual WWPN and WWNN gets set to 08 and 07, instead of 01 and 00. How do I resolve this issue?

Answer: Perform the following steps:

1. Clear all NIC partitions.
2. Reboot the server.
3. Partition the NIC again.
4. Deploy the server again with virtual I/O attributes.

Question: I deployed a configuration template on a server. What must I do if I want to edit some attributes of the same configuration template and then deploy it on another server?

Answer: It is recommended that you clone the configuration template, edit the attributes, and then deploy the cloned template on another server.

Logs

Question: How do I enable logging in OpenManage Essentials?

Answer: To enable logging:

1. Go to `C:\Program Files\Dell\SysMgt\Essentials\configuration` or the path where OpenManage Essentials is installed.
2. Open the `dconfig.ini` file using notepad.
3. In the [Logging] section, modify the following:

- Set LOG_ENABLED=true to enable logging.
- Set LOG_TO_FILE=true to write logs to a file.
- Type a path for LOG_FILE_PREFIX. For example, LOG_FILE_PREFIX=C:\windows\temp.
- If required, change the suffix of the file for LOG_FILE_SUFFIX=ome_log.txt.
- Set the log level for LOG_LEVEL_MIN. For example, LOG_LEVEL_MIN=debug.



NOTE: Setting the minimum log level (LOG_LEVEL_MIN) to debug or trace reduces the performance of OpenManage Essentials.

- Set the log level for LOG_LEVEL_MAX. For example, LOG_LEVEL_MAX=output.



NOTE: The maximum log level (LOG_LEVEL_MAX) must always be set to output.




NOTE: For more information about log severity levels, see the “Log Levels” section.

4. Close the file and restart all DSM services in the **Services** Microsoft Management Console.

Log Levels

Setting the log levels determines the range of message severity type you want to log. The following table describes the log message severity levels that you can assign to LOG_LEVEL_MIN and LOG_LEVEL_MAX.

Table 261. Log Levels

Severity Level	Description
Trace	Detailed information related to code flow.  NOTE: It is not recommended to set the minimum log level to trace unless instructed to do so by technical support.
Debug	Detailed information that may be useful when diagnosing problems.
Info	Information related to operational events.
Warning	An indicator that something unexpected happened or an indication of some problem in the near future. The software is still working as expected. Typically, related to configuration or network issues (time outs, retries, and so on).
Error	A problem resulting in the software being unable to perform some function.
Fatal	A serious error, indicating that the software may not be able to continue running.
Output	Information that needs to be output in situations where the logging system is not initialized.

By default, the minimum and maximum log message severity level are set to:

- LOG_LEVEL_MIN=info
- LOG_LEVEL_MAX=output

The default settings ensure that all messages with a severity of at least 'info' and at most 'output' are logged.

Backup and Restore

Question: After a backup and restore of the OpenManage Essentials database, I am unable to use the sample tasks and also the tasks that I created. What could be the reason?

Answer: The task configuration data is saved in the OpenManage Essentials database in an encrypted format. When a backup and restore is performed, the encrypted data becomes unusable. Therefore, you will have to recreate all tasks that you had created. Sample tasks will continue to remain unusable.

Troubleshooting

Question: What do I need to do if all SNMP traps from an ESXi 5 host show up in OpenManage Essentials as unknown?

Answer: You must change the hardware event source in the SNMP config on the ESXi 5 host from CIM to IPMI. Run the following commands:

```
vicfg-snmp.pl --username root --password <yourpassword> --server <yourserver> --hwsrc  
sensors
```

The output of the --show command would display the following:

Current SNMP agent settings:

Enabled : 1

UDP port : 161

Communities : public

Notification targets :

<myOMEServername>@162/public

Options :

EnvEventSource=sensors


Managing Device Group Permissions

The **Device Group Permissions** portal allows **OmeAdministrators** to grant users the permission to perform system updates and run remote tasks on select device groups.

Using the **Device Group Permissions** portal, **OmeAdministrators** can:


- Add users to the **OmeSiteAdministrators** role.
- Assign device groups to each user in the **OmeSiteAdministrators** role, allowing the user to perform system updates and run remote tasks on only the assigned device groups.


 **NOTE:** To effectively manage device group permissions, it is recommended that a member of the **OmeSiteAdministrators** role is removed from the **OmeAdministrators** and **OmePowerUsers** roles.


 **NOTE:** If a device group is not assigned to a user, it only restricts the user from performing system updates or running remote tasks on that device group. It does not hide or remove that device group from the device tree in the **Devices** portal.

The **Common Tasks** pane displays the **Edit Members of OmeSiteAdministrators** option that can be used to add or remove users from the **OmeSiteAdministrators** role.

The **Manage Device Group Permissions** pane displays the **OmeSiteAdministrators** in a tree-view format. If you select **OmeSiteAdministrators** at the root of the tree-view, the **User Overviews** are displayed in the right-side pane. If you select a user in the **OmeSiteAdministrators** tree-view, the right-side pane displays the *user name* and the **Device Groups for Tasks and Patch Targeting** section.

 **NOTE:** An **OmeSiteAdministrators** task target remains 'as is' when the task was created. If the **OmeAdministrators** change the **OmeSiteAdministrators** device group permissions, the task targets are not modified. Changing an **OmeSiteAdministrators** device group permissions does not change tasks the **OmeSiteAdministrators** created earlier.

 **NOTE:** Only Server, RAC, or custom device groups that are assigned to **OmeSiteAdministrators** are available to **OmeSiteAdministrators** for remote or system update tasks. To make any other device groups available to the **OmeSiteAdministrators** for remote or system update tasks, you must create a custom device group which includes other device groups and assign it to the **OmeSiteAdministrators**.

 **NOTE:** If a user in the **OmeSiteAdministrators** role is removed from the Windows user groups, the user is not removed from the **OmeSiteAdministrators** role automatically. You must remove the user from the **OmeSiteAdministrators** role manually through the **Edit Members of OmeSiteAdministrators** option.

Related link

[Permissions](#)

Adding Users to the OmeSiteAdministrators Role

 **NOTE:** Only **OmeAdministrators** are allowed to add users to the **OmeSiteAdministrators** role.

 **NOTE:** To effectively manage device group permissions, it is recommended that a member of the **OmeSiteAdministrators** role is removed from the **OmeAdministrators** and **OmePowerUsers** roles.

To add users to the **OmeSiteAdministrators** role:

1. Click **Settings** → **Permissions**.
The device group **Permissions** portal is displayed.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Edit Members of OmeSiteAdministrators**.
 - In the **Manage Device Group Permissions** pane, right-click **OmeSiteAdministrators**, and click **Edit Members of OmeSiteAdministrators**.

The **Edit Members of OmeSiteAdministrators** dialog box is displayed.

3. Type or select the domain name and user name in the appropriate fields, and click **Add**.
4. Select the user from the list and click **OK**.

The user is displayed in the **OmeSiteAdministrators** tree view in the **Manage Device Group Permissions** pane.


 **NOTE:** To restrict the user to perform system updates and remote tasks on specific device groups, you must assign the device groups to the user. See [Assigning Device Groups to a User](#).

Related link

[Permissions](#)


Assigning Device Groups to a User


 **NOTE:** Only OmeAdministrators are allowed to assign device groups to a user. Device groups can only be assigned to users who are members of the OmeSiteAdministrators role.

 **NOTE:** If a device group is not assigned to a user, it only restricts the user from performing system updates or running remote tasks on that device group. It does not hide or remove that device group from the device tree in the Devices portal.

To assign device groups to a user:

1. Click **Settings** → **Permissions**.
The device group **Permissions** portal page is displayed.
2. In the **Manage Device Group Permissions** pane, select the user to whom you want to assign device groups.
The **Device Groups for Tasks and Patch Targeting** section is displayed in the right-side panel.
3. In the device groups tree-view, select the check boxes appropriate to the device group(s) you want to assign to the selected user. If you want to remove a device group assignment that you made previously, clear the check boxes of the appropriate device groups.
4. Click **Apply**.

 **NOTE:** An OmeSiteAdministrators task target remains 'as is' when the task was created. If the OmeAdministrators change the OmeSiteAdministrators device group permissions, the task targets are not modified. Changing an OmeSiteAdministrators device group permissions does not change tasks the OmeSiteAdministrators created earlier.

 **NOTE:** Only Server, RAC, or custom device groups that are assigned to OmeSiteAdministrators are available to OmeSiteAdministrators for remote or system update tasks. To make any other device groups available to the OmeSiteAdministrators for remote or system update tasks, you must create a custom device group which includes other device groups and assign it to the OmeSiteAdministrators.

Related link

[Permissions](#)

Removing Users From the OmeSiteAdministrators Role

 **NOTE:** Only OmeAdministrators are allowed to remove users from the OmeSiteAdministrators role.

To remove users from the **OmeSiteAdministrators** role:

1. Click **Settings** → **Permissions**.
The device group **Permissions** portal page is displayed.
2. Perform one of the following:
 - In the **Common Tasks** pane, click **Edit Members of OmeSiteAdministrators**.
 - In the **Manage Device Group Permissions** pane, right-click **OmeASitedministrators**, and click **Edit Members of OmeSiteAdministrators**.

The **Edit Members of OmeSiteAdministrators** dialog box is displayed.

3. Clear the check box beside the user who you want to remove from the **OmeSiteAdministrators** role.
4. Click **OK**.
The user is removed from the **OmeSiteAdministrators** tree view in the **Manage Device Group Permissions** pane.

Related link

[Permissions](#)

OpenManage Mobile Settings

OpenManage Mobile is a systems management application that allows you to securely perform a subset of data-center monitoring and remediation tasks on one or more OpenManage Essentials consoles and/or integrated Dell Remote Access Controllers (iDRACs) using your Android or iOS device. Using OpenManage Mobile you can:

- Receive alert notifications from the OpenManage Essentials management system/server.
- View group, device, alert, and log information.
- Power on/off or restart a server.

This chapter provides information about the OpenManage Mobile settings that you can configure through the OpenManage Essentials console. It also provides information required to troubleshoot OpenManage Mobile.

 **NOTE:** For information on installing and using OpenManage Mobile, see the *OpenManage Mobile User's Guide* at Dell.com/OpenManageManuals.

Related links

[Enabling or Disabling Alert Notifications For OpenManage Mobile](#)

[Enabling or Disabling OpenManage Mobile Subscribers](#)

[Deleting an OpenManage Mobile Subscriber](#)

[Viewing the Alert Notification Service Status](#)


[Viewing the OpenManage Mobile Subscriber Information](#)

[Troubleshooting OpenManage Mobile](#)

Enabling or Disabling Alert Notifications For OpenManage Mobile

By default, OpenManage Essentials is configured to send alert notifications to the OpenManage Mobile application. However, alert notifications are sent from OpenManage Essentials only when a OpenManage Mobile user adds the OpenManage Essentials console to the OpenManage Mobile application. The **Enable Push Notifications** option in the **Settings** → **Mobile Settings** page allows you to enable or disable the OpenManage Essentials console from sending alert notifications to OpenManage Mobile subscribers.

 **NOTE:** omeAdministrator rights are required for enabling or disabling alert notifications for OpenManage Mobile.

 **NOTE:** For OpenManage Essentials to send alert notifications to OpenManage Mobile, make sure that the OpenManage Essentials server has outbound (HTTPS) Internet access. For more information, see “Proxy Settings” in [General Settings](#).

To enable or disable alert notifications for OpenManage Mobile:




1. In OpenManage Essentials, click **Settings** → **Mobile Settings**.
The **Mobile Settings** page is displayed.
2. Select or clear **Enable Push Notifications** to enable or disable sending alert notifications to OpenManage Mobile subscribers.
3. Click **Apply**.

Related link

[OpenManage Mobile Settings](#)

Enabling or Disabling OpenManage Mobile Subscribers

The check boxes in the **Enabled** column in the **Mobile Subscribers** list allow you to enable or disable transmission of alert notifications to OpenManage Mobile subscribers.

-  **NOTE:** omeAdministrator rights are required for enabling or disabling OpenManage Mobile subscribers.
-  **NOTE:** OpenManage Mobile subscribers may be automatically disabled by OpenManage Essentials if their mobile service provider push notification service indicates that the device is permanently unreachable.
-  **NOTE:** Even if an OpenManage Mobile subscriber is enabled in the Mobile Subscribers list, they can disable receiving alert notifications in their OpenManage Mobile application settings.

To enable or disable alert notifications to OpenManage Mobile subscribers:

1. In OpenManage Essentials, click **Settings** → **Mobile Settings**.
The **Mobile Settings** page is displayed.
2. In the **Mobile Subscribers** list, select or clear the **Enabled** check box to enable or disable alert notifications to the appropriate OpenManage Mobile subscribers.
3. Click **Apply**.

Related link


[OpenManage Mobile Settings](#)

Deleting an OpenManage Mobile Subscriber

Deleting an OpenManage Mobile subscriber removes the user from the **Mobile Subscribers** list, preventing the user from receiving alert notifications from the OpenManage Essentials console. However, the OpenManage Mobile user can re-subscribe to alert notifications from the OpenManage Mobile application at a later time.

-  **NOTE:** omeAdministrator rights are required for deleting an OpenManage Mobile subscriber.

To delete an OpenManage Mobile subscriber:

1. In OpenManage Essentials, click **Settings** → **Mobile Settings**.
The **Mobile Settings** page is displayed.
2. In the **Mobile Subscribers** list, click the delete icon  appropriate to the subscriber you want to delete.
The **Delete Subscription Confirmation** dialog box is displayed.
3. Click **Yes**.

Related link

[OpenManage Mobile Settings](#)

Viewing the Alert Notification Service Status

OpenManage Essentials forwards alert notifications to OpenManage Mobile subscribers through their respective device platform alert notification service. If the OpenManage Mobile subscriber has failed to receive alert notifications, you can check the **Notification Service Status** to troubleshoot alert notification delivery.

To view the status of the alert notification service, click **Settings** → **Mobile Settings**.

Related links


[OpenManage Mobile Settings](#)




[Notification Service Status](#)

Notification Service Status

The following table provides information about the **Notification Service Status** displayed in the **Settings** → **Mobile Settings** page.

Table 262. Notification Service Status

Status Icon	Status Description
	The service is running and operating normally.

Status Icon	Status Description
	 NOTE: This service status only reflects successful communication with the platform notification service. If the device of the subscriber is not connected to the Internet or a cellular data service, notifications will not be delivered until the connection is restored.
	The service experienced an error delivering a message which may be of a temporary nature. If the problem persists, follow troubleshooting procedures or contact technical support.
	The service experienced an error delivering a message. Follow troubleshooting procedures or contact support as needed.

Viewing the OpenManage Mobile Subscriber Information

After an OpenManage Mobile user successfully adds an OpenManage Essentials console, the user is added to the **Mobile Subscribers** table in the OpenManage Essentials console. The **Mobile Subscribers** table provides information about each OpenManage Mobile subscriber.

To view the mobile subscriber information, in OpenManage Essentials, click **Settings** → **Mobile Settings**.

Related links

[OpenManage Mobile Settings](#)


[Mobile Subscriber Information](#)

Mobile Subscriber Information

The following table provides information about the **Mobile Subscribers** table displayed in the **Settings** → **Mobile Settings** page.

Table 263. Mobile Subscriber Information

Field	Description
Enabled	Displays a check box you can select or clear to enable or disable alert notifications to an OpenManage Mobile subscriber.
Status	Displays the status of the subscriber, indicating whether the OpenManage Essentials console is able to send alert notifications successfully to the Alert Forwarding Service.
Status Message	Displays the status of the mobile device.
Username	Displays the name of the OpenManage Mobile user.
Device Id	Displays the unique identifier of the mobile device.
Description	Displays the description of the mobile device.
Filter	Displays the name of the filter the subscriber has configured for alert notifications.
Last Error	Displays the date and time the last error occurred when sending an alert notification to the OpenManage Mobile user.
Last Push	Displays the date and time the last alert notification was sent successfully from OpenManage Essentials to the Alert Forwarding Service.
Last Connection	Displays the date and time the user last accessed the OpenManage Essentials console through OpenManage Mobile.

Field	Description
Registration	Displays the date and time the user added the OpenManage Essentials console in OpenManage Mobile.
Delete	Displays a delete icon  that you can click to remove a subscriber from the Mobile Subscribers list.

Troubleshooting OpenManage Mobile

If OpenManage Essentials is unable to register with the Message Forwarding Service or successfully forward notifications, the following resolutions are available:

Table 264. Troubleshooting OpenManage Mobile

Problem	Reason	Resolution
OpenManage Essentials is unable to connect to the Dell Message Forwarding Service. [Code 1001/1002]	Outbound Internet (HTTPS) connectivity is lost.	Using a web browser, determine if outbound Internet connectivity is available. If connectivity is lost, perform standard network troubleshooting steps: <ul style="list-style-type: none"> • Verify if the network cables are connected. • Verify the IP address and DNS server settings. • Verify if the firewall is configured to allow outbound traffic. • Verify if the ISP network is operating normally.
	Proxy settings are incorrect.	Set proxy host, port, username, and password as required. For more information, see "Proxy Settings" in General Settings .
	Message Forwarding Service is temporarily unavailable.	Wait for the service to become available.
The Message Forwarding Service is unable to connect to a device platform notification service. [Code 100-105, 200-202, 211-212]	The platform provider service is temporarily unavailable to the Message Forwarding Service.	Wait for the service to become available.
The device communication token is no longer registered with the platform provider service. [Code 203]	The OpenManage Mobile application has been updated, restored, uninstalled, or the device operating system has been upgraded or restored.	Reinstall OpenManage Mobile on the device or follow the OpenManage Mobile troubleshooting procedures specified in the <i>OpenManage Mobile User's Guide</i> and reconnect the device to OpenManage Essentials. If the device is no longer connected to OpenManage Essentials, remove the subscriber.
The OpenManage Essentials registration is being rejected by the Message Forwarding Service. [Code 154]	An obsolete version of OpenManage Essentials is being used.	Upgrade to a newer version of OpenManage Essentials.

Related link

[OpenManage Mobile Settings](#)

Settings — Reference

In the Settings page, you can configure the OpenManage Essentials console. You can set the SMTP and proxy server information, adjust session timeout, database maintenance schedules, restart services, create custom URL menu items, enable or disable internal alerts, observe daylight savings time, and enable or disable the ActiveX features.

 **NOTE:** After modifying the general settings, click **Apply** to save the changes. Navigating to another portion of the console without clicking **Apply** resets the settings to the previously saved preferences.

Related links

[Alert Settings](#)
[Custom URL Settings](#)
[Deployment Settings](#)
[Device Tree Settings](#)
[Discovery Settings](#)
[Feature Usage Settings](#)
[Email Settings](#)
[General Settings](#)
[OpenManage Mobile Settings](#)
[Task Settings](#)
[Warranty Notification Settings](#)
[Purge Download Settings](#)
[Permissions](#)

Alert Settings

Table 265. Alert Settings

Field	Description
Enable Internal Health Alerts	Select the check box to enable internal health alerts. When enabled, OpenManage Essentials generates internal alerts when the global health status of the device changes.
Enable Internal Connection Status Alerts	Select the check box to enable internal connection status alerts. When enabled, OpenManage Essentials generates internal alerts when the connection status of the device changes.
Alert Popup Notification Settings	
Enable Alert Popup Notifications	Select the check box to enable pop-up notifications to be displayed when an alert is received.
Seconds between popup notifications	Select the time interval between each alert pop-up notification.
SNMP Listener Settings	
Support V1/V2c Traps	Select the option to use Windows SNMP Trap service for receiving the traps.
Support V1/V2c/V3 Traps	Select the option to use dedicated Net SNMP trap reception port for receiving the traps.

Field	Description
Dedicated Trap listening port	Enter the SNMP trap reception port. By default, the dedicated trap reception port is 162.

Custom URL Settings

Table 266. Custom URL Settings

Field	Description
Name	Displays the name assigned to the URL.
Device Group	Displays the device group associated with the URL.
Custom URL	Displays the URL.
Description	Displays the description provided for the custom URL.
Date Created	Displays the date the URL was created.
Date Updated	Displays the date the URL was updated.

Related links

[Creating a Custom URL](#)

[Launching the Custom URL](#)

Deployment Settings



The fields displayed in the **Deployment Settings** page are described in the following table.

Table 267. Deployment Settings

Field	Description
File Share Settings	
Domain \ Username	User name to access the file share.
Password	Password to access the file share.
File Share Status	Indicates the status of the deployment file share configuration.
Allow using file share for Device Configuration feature on server	Allows using file share for device configuration features on the server.
Auto Deployment Settings	
Enable auto deployment for recently discovered devices	Select to allow OpenManage Essentials to deploy a configuration template to devices that will be discovered later.
Run auto deployment every xx Minutes	Set the time interval at which you want to attempt the configuration deployment on devices that will be discovered later.

Device Tree Settings


Table 268. Device Tree Settings


Field	Description
Always display RAC device name under RAC group	Select the check box to display the RAC name (RAC DNS name or instrumentation name) of the iDRAC in the device tree, portals, and wizards.  NOTE: The RAC name is displayed only if you have discovered the iDRAC with the WS-Man protocol. Otherwise, the system name is displayed instead of the RAC name.
Identify devices with lost connection in device tree	Select the check box to display the  icon in the device tree and portals for devices that are not reachable.

Discovery Settings

The **Discovery Settings** page enables you to configure the type of wizard you want to use for discovering devices. The fields displayed in the **Discovery Settings** page are described in the following table.

Table 269. Discovery Settings


Field	Description
Standard Wizard	If selected, the Discover Devices wizard displays a list of protocols for discovering devices.
Guided Wizard	If selected, the Discover Devices wizard displays a list of device types and the required protocols for discovering and managing the selected devices. After the required protocol configurations are completed, by default, this wizard runs both discovery and inventory.  NOTE: Discovery of Dell EMC storage arrays is not supported by the Guided Wizard.
Skip ICMP ping during discovery	If selected, the ICMP Configuration settings will be disabled from the Discover Devices wizard. By selecting this option, ICMP ping is skipped during discovery and inventory of the devices, system updates, configuration and deployment tasks.
Discover the selected Device Types only	In OpenManage Essentials 2.5, this option is enabled by default. If selected, this option allows device-type discovery in the guided wizard.

Field	Description
	 NOTE: The device range that was discovered in OpenManage Essentials version 2.2 and earlier may have discovered both chassis and iDRAC using WS-MAN protocol. In OpenManage Essentials 2.5, if Discover the selected Device Types only option is enabled in Discovery settings, then only the specific device selected in the guided wizard will be discovered and other devices are classified as unknown devices. For example: Selecting iDRAC device type with WS-MAN protocol will discover only iDRAC devices using WS-MAN protocol.

Feature Usage Settings

In OpenManage Essentials version 2.5, to understand and to improve the most used features, the following information is collected when you choose to join the OpenManage Essentials Customer Experience Improvement Program:

- The number of devices being monitored.
- The distinct type of devices being monitored. For example, servers, chassis, switches, and storage.
- The number of servers with the **Server Configuration Management** license installed.
- The number of servers that are discovered by using in-band discovery methods.
- The type and number of tasks created.
- The number of:
 - Configured discovery and excluded discovery ranges
 - Alerts received and the alert actions
 - Created configuration templates and baselines
 - Configured virtual identity pools
 - Managed catalogs

 **NOTE:** No personal information to identify or to contact you are collected during this activity.



Email Settings

Table 270. Email Settings

Field	Description
SMTP Server Name or IP Address	Enter the SMTP server name or IP address.
Use Credentials	Enable the user credentials.
Domain \ User name	Enter the domain and user name.
Password	Enter the user password.
Port	Check Use Default to use the default port number or manually add the port number.
Use SSL	Enable this check box to use SSL.
Logging	Select to enable or disable logging based on your preference.

General Settings


Table 271. General Settings

Field	Description
Console Session Timeout	Amount of user-inactive time that passes before the console automatically logs the user out.
Database Maintenance Execution Schedule	<p>The date and time when the database maintenance activity will begin.</p> <p> NOTE: It is recommended not to run or schedule any task (discovery, inventory, status polling, and so on) during database maintenance, as the console is less responsive during database maintenance.</p>
Restart All OpenManage Essentials Services	<p>Restarts the services associated with OpenManage Essentials.</p> <p> NOTE: It is recommended to have discovery, inventory, status polling, and other tasks completed before restarting the OpenManage Essentials services.</p>
Security Settings (ActiveX)	
Allow MIB Import Utility Launch	Installs and runs an ActiveX component on the client machine to launch the MIB Import Utility.
Allow Remote Desktop Launch	Installs and runs an ActiveX component on the client machine to launch remote desktop sessions.
Allow Troubleshooting Tool Launch	Installs and runs an ActiveX component on the client machine to launch the Troubleshooting Tool.
ActiveX Status	Displays the ActiveX status. Click Refresh Status to refresh the ActiveX status.
Time Zone Settings	
Observe Daylight Savings Time for Server Selected Region	Click this check box to enable adjusting the scheduled date and time values based on the server's time zone. Adjusting the server's time zone setting changes the settings in OpenManage Essentials. Enabling this option adjusts the date and time values of scheduled items when daylight savings begin or ends.
Client Time Zone	Displays the time zone and UTC offset of the client's time zone.
OME Server Time Zone	Displays the time zone and UTC offset of the server's time zone.
OME Server Daylight Savings Status	Displays the current daylight savings time status of the server's time zone and offset of daylight savings time. It also displays whether the server's time zone is observing daylight savings or is in standard time zone time.
Proxy Settings (used for System Update and Warranty)	
Use Proxy Settings	Enable the use of proxy settings for internet access for System Update and Warranty.
Proxy Server Address or Name	The IP address or server name of the proxy server. Check the browser's proxy LAN settings, or ask your network administrator if unsure.
Domain \ User name	The domain and user name of the proxy user.

Field	Description
Password	User's proxy password.
Proxy Port Number	The port number to access the proxy server. Check the browser's proxy LAN settings, or ask your network administrator if unsure.
Test Connection	Click to test connection to the internet with the proxy credentials.
KACE Appliance Settings	
KACE Appliance URL	The URL of the KACE appliance.
Test URL	Click to test connectivity to the KACE appliance.

Task Settings

Table 272. Task Settings

Field	Description
Task Execution History Settings	
Task Execution History Records to be Retained	<p>Select the number of records to load in the Task Execution History.</p> <p> NOTE: Older task execution history records are purged when this limit is exceeded, except for discovery, inventory, status polling, importing catalog for system update, device configuration inventory, updating OME internal component, deploying configuration to undiscovered devices tasks.</p>
Task Popup Notification Settings	
Enable Task Popup Notifications	Select the check box to enable pop-up notifications to be displayed when a task is completed.
Seconds between popup notifications	Select the time interval between each task pop-up notification.

Warranty Notification Settings

The following table provides information about the fields displayed in the **Settings → Warranty Notification Settings** page.

Table 273. Warranty Notification Settings

Field	Description
Warranty Email Notifications	
Enable Warranty Email Notifications	Enables or disables the sending of warranty email notifications.
To	The email addresses of the recipients of the warranty notification email. Each email address must be a valid email address. Multiple email addresses must be separated using a semicolon.
From	The email address from which the warranty notification email is to be sent. Only one email address must be provided. The email address must be a valid email address.

Field	Description
All Devices with x days or less of warranty	Determines which devices to include in the warranty notification email. Devices with warranty less than or equal to the specified days are included in the warranty notification email.
Include Expired Warranties	Specifies if devices with expired warranty (0 days) or no warranty information should be included in the warranty email notification.
Send email every x days	The duration between successive warranty email notifications. An update to this field takes effect only after the next warranty email notification is sent.
Next Email Will Send On	The date and time at which the next warranty notification email is to be sent. You can configure this field to set when the next warranty notification email is to be sent. After an email notification is successfully sent, this field is updated automatically based on the setting in the Send email every x days field.
Email Settings	Opens the E-mail Settings page where you can configure the SMTP email server.
Warranty Scoreboard Notifications	
Enable Warranty Scoreboard Notifications	Enables or disables the display of the warranty notifications icon in the OpenManage Essentials heading banner. The warranty notification icon is displayed only if a device has warranty less than or equal to the days specified in All Devices with x Days or less of warranty .
All Devices with x Days or less of warranty	Determines which devices to include in the warranty notification email. Devices with warranty less than or equal to the specified days are included in the warranty notification email.
Include Expired Warranties	Specifies if devices with expired warranty (0 days) or no warranty information should be included in the Device Warranty Report .
Warranty Popup Notification Settings	
Enable Warranty Popup Notification	Enables or disables the display of the warranty popup notifications in the console. The warranty popup notification is displayed only if a device has warranty less than or equal to the days specified in All Devices with x Days or less of warranty .
Warranty Update Settings	
Enable Warranty Updates	Enables or disables the checking of warranty information of the discovered devices on the support site.
Update warranty every x days	The duration between successive warranty update checks.
Next warranty update will be on	The date and time at which the next warranty updates are checked. You can configure this field to set when the next warranty updates are checked. After the warranty information is successfully checked, this field is updated automatically based on the setting in the Update warranty every x days field.

Related links

- [Configuring Warranty Email Notifications](#)
- [Configuring Warranty Scoreboard Notifications](#)

Permissions

The following is the description of the panels and fields displayed in the **Device Group Permissions** portal.

Common Tasks

The **Common Tasks** pane displays the **Edit Members of OmeSiteAdministrators** option that you can use to add or remove a user from the **OmeSiteAdministrators** role.

Manage Device Group Permissions

The **Manage Device Group Permissions** pane displays the **OmeSiteAdministrators** in a tree-view format. The **User Overviews** are displayed in the right-side pane when you click **OmeSiteAdministrators** in the **Manage Device Group Permissions** pane. The following are the fields in **User Overviews**:

Table 274. Manage Device Group Permissions

Field	Description
User Type	Displays if the member is a user or user group.
Domain	Displays the domain of the user.
Name	Displays the name of the user.

Device Groups for Tasks and Patch Targeting

The **Device Groups for Tasks and Patch Targeting** section is displayed in the right-side pane when you click a *user name* in the **Manage Device Group Permissions** pane. This section displays the device groups in a tree-view format.

Related links

- [Managing Device Group Permissions](#)
- [Adding Users to the OmeSiteAdministrators Role](#)
- [Assigning Device Groups to a User](#)
- [Removing Users From the OmeSiteAdministrators Role](#)

Purge Download Settings

The **Purge Download Settings** page allows you to configure the settings for automatic purging of downloaded BIOS, firmware, driver, and application files.

The following table provides information about the fields displayed in the **Settings** → **Purge Download Settings** page.

Table 275. Purge Download Settings

Field	Description
Enable purging of downloaded files	Select to allow purging of the BIOS, firmware, drivers, or application files that are downloaded by OpenManage Essentials.
Size limit of the downloads folder (GB)	Select the size limit of the folder to which OpenManage Essentials downloads the files that are required for applying system updates or remote tasks. By default, the downloaded files are saved in the <install location>\Essentials\System Update folder. Files will be automatically purged from the

Field	Description
	downloads folder (<install location>\Essentials\System Update) when the folder size reaches the defined size limit. (Range: 5 GB to 20 GB; Default: 20 GB)
Approximate size of the downloaded files to be purged	Select the approximate size of the downloaded files that you want to purge. Files will be purged until the total size of the purged files reaches or exceeds the approximate size that you have defined. (Range: 1 GB to 4 GB; Default: 4 GB)

Related link

[Configuring automatic purging of downloaded system update files](#)

Logs — Reference

From tools you can:

- View User Interface Logs
- View Application Logs



Figure 36. Toolbar — Export

Export Discovery Logs to File System — Export the logs that were generated while discovering devices.

User Interface Logs

Table 276. User Interface Logs

Field	Description
Enabled	Enable or disable logging of User Interface. Disable to increase performance.
Log Asynchronous Calls	Enable or disable logging for threading and asynchronous update method calls. Turn on both Log Asynchronous Calls and Informational to view update calls.
Informational	Enable or disable logging of behaviors that are marked with a severity of General Information .
Warning	Enable or disable logging of behaviors that are marked with a severity of Warning .
Critical	Enable or disable logging of behaviors that are marked with a severity of Critical .
Clear	Clear the user interface log grid.
Export	Export the user interface log to file (.CSV, .HTML, .TXT, and .XML supported).
Severity	The severity of the recorded deviation in user interface behavior.
Start Time	The time at which this behavior occurred.
Source	The source of the behavior.
Description	More information on the behavior.

Application Logs

Table 277. Application Logs





Field	Description
Severity	The severity of the recorded deviation in application's behavior.
Time	The time at which this behavior occurred.
Message	Information on the behavior.

Dell EMC Solutions

The **Dell EMC Solutions** portal provides a list of links to other tools associated with OpenManage Essentials. This page provides information about the tool, detects if the tool is installed, and enables you to launch the tool if it is installed.

 **NOTE:** You may require ActiveX to detect some extensions. To enable ActiveX, see [General Settings](#) in the Settings page.

Table 278. Dell EMC Solutions

Field	Description
Name	Displays the name of the tool.
Description	Displays the description of the tool.
Action	<p>If the tool is installed and ActiveX is enabled, a link is displayed. You can click the link to launch the tool.</p> <p> NOTE: For the inventory collector component, the Action column may display the following:</p> <ul style="list-style-type: none"> • Up-to-date — Indicates that OpenManage Essentials has the latest version of inventory collector component. • Update — Indicates that a newer version of the inventory collector component is available. Click to download the inventory collector component for both Windows and Linux in the background.
Version	<p>Displays the version of the tool.</p> <p> NOTE: For the inventory collector component, the Version column may display the following:</p> <ul style="list-style-type: none"> • Up-to-date icon  — Indicates that OpenManage Essentials has the latest version of the inventory collector. • Warning icon  — Indicates that OpenManage Essentials does not have the latest version of the inventory collector.
Additional Information	Click the ? icon to see more information about the product.

Related link

[Updating the inventory collector component](#)

Right-Click Actions

The following tables lists all the right-click actions that are available in OpenManage Essentials.

 **NOTE:** The right-click options displayed in OpenManage Essentials are dependent on your access privilege. You must have administrator access to see all the options.


Schedule View

Table 279. Schedule View

Action	Description
Create New Task	Displays the following options: <ul style="list-style-type: none"> • Server Power Options • Deploy Server Administrator Task • Command Line Task
Export Calendar	Allows you to export the calendar in an .ics file format. You can import the ics file into Microsoft Outlook.

After you create a task, you can right-click the task to display the following options:

Table 280. Action Items

Actions	Description
Edit	Allows you to edit the task.
Delete	Allows you to delete the task.
Run Now	Allows you to run the task immediately.
View	Allows you to view the details of the task.
Deactivate Task Schedule	Deactivates a task's schedule. This flag determines if the task runs or not in the future. <div>  NOTE: If you right-click a deactivated task, an Activate Task Schedule option is displayed. </div>
Clone	Allows you to clone the task with the same details.
Export Calendar	Allows you to export the calendar in an ics file format. You can import the ics file into Microsoft Outlook.

Device Status

Table 281. Device Status

Action	Description
IP address or device name	Displays the IP address or name of the device.
Application Launch	Select to launch an associated application.

Action	Description
Device Configuration	<ul style="list-style-type: none"> • Refresh Device Configuration Inventory — Refresh the configuration inventory of the device. • Add Devices to Repurpose and Bare Metal Device Group — Add the device to the Repurpose and Bare Metal Device Group. • Associate to Template — Associate the device to a device configuration template. • Create Template — Create a device configuration template from the device. • Deploy Template — Deploy a device configuration template on the device. • Reclaim Identities — Reclaim deployed virtual I/O identity attributes from the device. • Replace Server — Replace a production server from the backup profile.
Troubleshoot	If the Troubleshooting Tool is installed, then select this option to launch the Troubleshooting Tool. The Troubleshooting Tool is disabled by default. To enable the Troubleshooting Tool, see Settings — Reference .
Refresh Inventory	Select to run inventory on the device.
Refresh Status	Select to run a status check on the device.
Add to New Group	Select to add the device to a group.
Add to Existing Group	Select to add the device to an existing group.
Ignore All Alerts from Device	Select to ignore all alerts from the device.
Exclude Range	Select to remove the device from the discovery and inventory range.
Delete	Select to remove the device information.

Associate Catalog Baseline

To associate custom device groups with a catalog baseline, right-click a custom device group and select **Associate Catalog Baseline**.

Table 282. Associate Catalog Baseline



Action	Description
Catalog Baselines	
List of Catalog Baselines	Select a catalog baseline from a list of available catalog baselines.
Create Catalog Baseline	
Baseline Name	Type to change the baseline name.
Use repository manager file	Click Browse to navigate the file system and select a repository manager file.
Import now	Select to import the catalog baseline.

Discovery Range Summary

Managing Include Ranges

Right-click the IP address or group to view the following options:

Table 283. Managing Include Ranges

Action	Description
Edit	Select to edit discovery range configuration.
Rename	Select to rename the range.  NOTE: This option is only displayed if you right-click an IP address.
Add Discovery Ranges to <Group Name>	Select this option to add additional ranges to an existing group.  NOTE: This option is only displayed if you right-click a group.
Delete	Select to delete a range.
Disable	Select to disable a range.
Perform Discovery Now	Select to do the discovery.
Perform Discovery and Inventory Now	Select to do the discovery and inventory.
Perform Status Polling Now	Select to start the status polling task for the discovered server or device.
Perform Inventory Now	Select to perform the inventory.
Export Range(s)	Select to export the discovery range as a .csv file.

View Filters

Table 284. View Filters

Action	Description
Edit	Select to edit the alert action or alert filter.
View Summary	Select to view all the systems that are critical.
Rename	Select to rename action or alert filter.
Clone	Select to create a copy of an action or alert filter.
Delete	Select the alert to delete the alerts.

Alerts

Table 285. Alerts

Action	Description
Details	Select to view the details of alerts.
Device Details	Select to view the device details.

Action	Description
Device Application Launch	Select to launch the console associated with the device.
Acknowledge	Select to set or clear alerts.
Delete	Select to delete alerts.
Ignore	Select to ignore alert filter action on the selected device or all devices. You can also use this option to ignore all alerts from the selected device.
Export	Select to export alert information in a CSV or HTML format.

Remote Tasks

Table 286. Remote Tasks

Action	Description
Edit	Select to edit the task.
Delete	Select to delete the task.
Run	Select to run the task immediately.
View	Select to view the task.
Activate Task Schedule	Select to activate the task schedule.
Clone	Select to create a copy of a task.

Custom URL

Table 287. Custom URL

Action	Description
Edit	Select to edit the URL.
Delete	Select to delete the URL.
Export	Select to export the information about the URL

System Update Tasks

Table 288. System Update Tasks

Action	Description
Delete	Select to delete the task.
Run	Select to re-run a task that is already complete, but did not update some of the components.
View	Select to view the task.
Export	Select to export the system update task information.
Stop	Select to stop the task.

Attributes Tab

Table 289. Attributes Tab

Action	Description
Check	Select the selected attributes.
Uncheck	Clear the selected attributes.
Export	Export all the attributes displayed in the Attributes tab.

Templates

Table 290. Templates

Action	Description
Deploy	Deploy the selected device configuration template.
Clone	Clone the selected device configuration template.
Rename	Rename the selected device configuration template.
Delete	Delete the selected device configuration template.
Export Template	Export the selected device configuration template.

Compute Pools

Repurpose and Bare Metal

Table 291. Repurpose and Bare Metal

Action	Description
Create Compute Pool	Create a compute pool.

Compute Pool

Table 292. Compute Pool

Action	Description
Deploy	Deploy a device configuration template.
Edit	Edit the compute pool.
Unlock	Unlock the compute pool.
View	View the compute pool wizard.
Rename	Rename the compute pool.
Delete	Delete the compute pool.

Action	Description
Replace Server	Replace a server with another server from within the same compute pool.

Devices

Table 293. Devices

Action	Description
Refresh Device Configuration Inventory	Refresh the configuration inventory of the device.
Remove Devices from Repurpose and Bare Metal Devices Group	Remove devices that are currently in the Repurpose and Bare Metal device group.
Create Template	Create a device configuration template from the server.
Reclaim Identities	Reclaim the virtual I/O identities of the server.
Remove from Pool	Remove a server from the compute pool.
Replace Server	Replace a server with another server from within the same compute pool.

Virtual Input-Output Pools

Virtual I/O Pool

Table 294. Virtual I/O Pool

Action	Description
Create Virtual I/O Pool	Create a virtual I/O pool.
Edit	Edit the virtual I/O pool.
View	View the virtual I/O pool wizard.
Rename	Rename the virtual I/O pool.
Delete	Delete the virtual I/O pool.

Devices with Identities

Table 295. Device with Identities

Action	Description
View Identities	View the deployed and assigned virtual I/O identities of a device.
Reclaim the Assigned Identities	Reclaim the assigned virtual I/O identities of a device.
Reclaim the Deployed Identities	Reclaim the deployed virtual I/O identities of a device.
Export	Export the details in an HTML, CSV, Text, or XML format.

Compliance by Template

Table 296. Compliance by Template

Action	Description
Associate Devices	Deploy the selected device configuration template.
Edit	Displays the attributes of the selected device configuration template in the right pane for editing.
Clone	Clone the selected device configuration template.
Rename	Rename the selected device configuration template.
Delete	Delete the selected device configuration template.
Export Template	Export the selected device configuration template.

Device Compliance

Table 297. Device Compliance

Action	Description
View Compliance Details	View the compliance details for the selected device.
Associate to Different Template	Associate the selected device to another configuration template.
Run Inventory Now	Run the device configuration inventory for the selected device.
Export	Export the device compliance report as an HTML file.

Tutorials

You can use these tutorials to complete the setup options when configuring OpenManage Essentials for the first time.

In the **Tutorials** tab, click **First Time Setup** to view the following configuration information:

- SNMP Configuration
- SNMP—Open Services Console
- SNMP—Open SNMP Properties
- Install SNMP Tools—Windows Server 2012 and later
- SNMP Security Settings
- SNMP Trap Settings
- Install OpenManage Server Administrator
- Enable Network Discovery—Windows Server 2008 and later
- Firewall Configuration
- Protocol Support Matrix
- Discover Devices

You can view the following tutorials:

- Upgrade to OpenManage Essentials 2.5
- Discover and Monitor 12G Servers without OpenManage Server Administrator
- Linux Configuration for SNMP and OpenManage Server Administrator
- SNMP Configuration using Group Policies
- Configuring ESX 4.x for Discovery and Inventory
- Configuring ESXi 4.x and 5.0 for Discovery and Inventory
- Device Group Permissions Tutorial

Using OpenManage Essentials Command Line Interface

Launching the OpenManage Essentials Command Line Interface

Click **Start** → **All Programs** → **OpenManage Applications** → **Essentials** → **Essentials Command Line Interface**.

Creating an input file for Discovery Profile

CLI commands that create discovery ranges or discovery groups require an XML-based file that defines the parameters for discovery protocols such as SNMP, WMI, Storage, WS-Man, SSH, and IPMI. This file defines which protocols are used and the parameters for each of the protocols. The file can be modified using an XML editor or a text editor. The **DiscoveryProfile.xml** file is placed at **C:\Program Files\Dell\SysMgt\Essentials\Tools\CLI**. Edit the .XML file and rename it to create multiple discovery profiles. You cannot store passwords for WMI, IPMI, WS-Man, EMC, and SSH protocols in the .XML file. The OpenManage Essentials CLI commands allow you to specify passwords in the command-line argument using the following commands:

- `-wmiPassword<secure password>`
- `-ipmiPassword<secure password>`
- `-wsmanPassword<secure password>`
- `-emcPassword<secure password>`
- `-sshPassword<secure password>`
- `-SNMPv3AuthenticationPassword<secure password>`
- `-SNMPv3EncryptionPassword<secure password>`

 **NOTE: Passwords are not allowed in clear text. If you attempt to use clear text for the password values, the CLI command fails to run.**

The `<secure password>` argument must be a secure password. To generate a secure password that can be reused in PowerShell scripts, run the following (or a similar command) from within a PowerShell window:

To prompt the user for a password; read in and convert it to a secure string:

```
PS> $password = Read-Host 'Enter password:' -AsSecureString
```

To save the password, as a secure string, to the file system:

```
PS> $password | ConvertFrom-SecureString | Set-Content c:\tmp\password.txt
```

The two earlier PowerShell commands convert a password to a secure string that is then saved in a file. This secure password can subsequently be used in other PowerShell scripts that involve OpenManage Essentials CLI commands. For example:

To read the secure password from the file and assign it to a variable:

```
PS> $passwordFile = convert-path c:\tmp\password.txt
```

```
PS> $wsmanpassword = Get-Content $passwordFile | ConvertTo-SecureString
```

To use the secure string in all the password variables in the OpenManage Essentials CLI commands:


```
PS> Add-DiscoveryRange -Range 10.36.0.48 -Profile samples\DiscoveryProfile.xml -WSManPassword $wsmanpassword
```

An example of the profile.xml file is outlined as follows:

 **NOTE:** If you discover iDRAC using WS-Man, and if you are using secure mode where a certificate file is required to be on the local system, specify the entire path to the certificate file. For example, `c:\192.168.1.5.cer`.

Specifying IPs, ranges, or host names by using XML or CSV files

You must specify ranges during discovery, inventory, and status tasks. A range in this instance is defined either as an individual IP address, a hostname, or a range of IPs such as 192.168.7.1-50 or 10.35.0.*. Add ranges, IPs, or host names either to an XML or CSV-based input file and then read the file by specifying it on the command line using the `-RangeList` or `-RangeListCSV` argument. A sample .xml file (`RangeList.xml`) and .csv file (`RangeList.csv`) are placed in the **samples** folder at `C:\Program Files\Dell\SysMgt\Essentials\Tools\CLI\Samples`. To create multiple input files, edit and rename either the XML or CSV file.

 **NOTE:** If you are creating discovery range groups, then each group can only have one corresponding subnet. The subnet for a group is read from the `DiscoveryProfile.xml` file and not from the `RangeList.xml` or `RangeList.csv` file. If required, you can create multiple groups for each subnet.

An example of the `RangeList.xml` file is outlined as follows:

An example of the `RangeList.csv` is outlined as follows:

Table 298. Examples of RangeList.csv

Name	SubnetMask
192.168.10.*	255.255.255.0
192.168.10.1-255	255.255.255.0
192.168.1-2.*	255.255.255.0
10.35.*.1-2	255.255.255.0
192.168.2.1	255.255.224.0
192.168.2.2	255.255.254.0
192.168.3.3	255.255.128.0
192.168.3.4	255.255.128.0

Specifying input files in PowerShell

To use input files in PowerShell, specify the location of the file in the command line. By default, OpenManage Essentials CLI starts at the following directory:

```
PS C:\Program Files\Dell\SysMgt\Essentials\Tools\CLI>
```

If you are running commands from the default CLI directory, with commands located in the directory one level from it (`\samples`), you can use either of the following methods of specifying the path to the input files:

- Enter the entire path name in quotes. For example, `Add-DiscoveryRange -Profile "C:\Program Files\Dell\SysMgt\Essentials\Tools\CLI\Samples\DiscoveryProfile.xml"`.
- Use a period (`.`) to retrieve the file located in the current directory, or `\directory` to retrieve the file located one level from the current directory. For example, `Add-DiscoveryRange -Profile .\samples\DiscoveryProfile.xml`.

Command Line Interface commands

Access to CLI commands in the OpenManage Essentials is dependent on your access privilege. If your user ID belongs to the **OMEAdministrators** group, you can access all the CLI commands. If your user ID belongs to the **OMEUsers** group, then you cannot delete or modify any data using the CLI and a warning message is displayed.

Creating a discovery range

Description: The `Add-DiscoveryRange` command allows you to create a new discovery range. The command references an .xml file (`DiscoveryProfile.xml`) which is a protocol definition associated with the discovery range. Enter the ranges either using an XML file, CSV file, or by specifying the range. For more information about `DiscoveryProfile.xml`, `RangeList.xml`, and `RangeList.csv` files, see [Creating a Discovery Profile Input File](#) and [Specifying IPs, Ranges, or Host Names Using XML or CSV Files](#).

Commands:

- `PS> Add-DiscoveryRange -Profile <DiscoveryProfile.xml> -Range <range>`
- `PS> Add-DiscoveryRange -Profile <DiscoveryProfile.xml> -RangeList <RangeList.xml>`
- `PS> Add-DiscoveryRange -Profile <DiscoveryProfile.xml> -RangeListCSV <RangeList.csv>`

Examples:

- `PS> Add-DiscoveryRange -Profile .\Samples\DiscoveryProfile.xml -Range 10.35.0.124`
- `PS> Add-DiscoveryRange -Profile .\Samples\DiscoveryProfile.xml -RangeList .\Samples\RangeList.xml`
- `PS> Add-DiscoveryRange -Profile .\Samples\DiscoveryProfile.xml -RangeListCSV .\Samples\RangeList.csv`

Editing a discovery range

Description: The `Set-ModifyDiscoveryRange` command allows to edit existing discovery ranges. This command targets the existing specified discovery range(s) and replaces the protocol information with the information specified in the `DiscoveryProfile.xml` file. For more information about the `DiscoveryProfile.xml` and `RangeList.xml` files, see [Creating a Discovery Profile Input File](#) and [Specifying IPs, Ranges, or Host names Using XML or CSV Files](#).

Commands:

- `PS> Set-ModifyDiscoveryRange -Profile <DiscoveryProfile.xml> -Range <range>`
- `PS> Set-ModifyDiscoveryRange -Profile <DiscoveryProfile.xml> -RangeList <RangeList.xml>`

Examples:

- `PS> Set-ModifyDiscoveryRange -Profile .\Samples\DiscoveryProfile.xml -Range 10.35.1.23`
- `PS> Set-ModifyDiscoveryRange -Profile .\Samples\DiscoveryProfile.xml -RangeList .\Samples\RangeList.xml`

Removing a discovery range

Description: The `Remove-DiscoveryRange` command allows you to remove a discovery range. Enter the ranges either using an XML file or by specifying the range. For more information about the `RangeList.xml` file, see [Specifying IPs, Ranges, or Host Names Using XML or CSV Files](#).

Commands:

- `PS> Remove-DiscoveryRange -Range <range>`
- `PS> Remove-DiscoveryRange -RangeList <rangelist.xml>`

Examples:

- `PS> Remove-DiscoveryRange -Range 10.35.0.1, 10.120.1.2`
- `PS> Remove-DiscoveryRange -RangeList .\Samples\RangeList.xml`

Creating a discovery range group

Description: The `Add-DiscoveryRangeGroup` command allows you to create a discovery range group. A discovery range group can either contain a range of IPs, individual IPs, or host names under it. This enables you to modify protocols settings for the group

and all the ranges it contains. You can maintain different sets of protocols for different types of devices in your network. With ranges not in a group, you have to edit each range individually to change the protocols which are active, the time out or retry values, or credentials used with each protocol. Each discovery range group can only have one corresponding subnet. The subnet for a group is read from the **DiscoveryProfile.xml** file and not from the **Rangelist.xml** or **RangeList.csv** file. If required, create multiple groups for each subnet. For more information about **DiscoveryProfile.xml**, **Rangelist.xml**, and **RangeList.csv** files, see [Creating a Discovery Profile Input File](#) and [Specifying IPs, Ranges, or Host names Using XML or CSV Files](#).

Command:

- `PS> Add-DiscoveryRangeGroup -Profile <DiscoveryProfile.xml> -GroupName <group name> -RangeList <Rangelist.xml>`
- `PS> Add-DiscoveryRangeGroup -Profile <DiscoveryProfile.xml> -GroupName <group name> -RangeListCSV <Rangelist.csv>`

Examples:

- `PS> Add-DiscoveryRangeGroup -Profile .\Samples\DiscoveryProfile.xml -GroupName Group1 -RangeList .\Samples\rangelist.xml`
- `PS> Add-DiscoveryRangeGroup -Profile .\Samples\DiscoveryProfile.xml -GroupName Group1 -RangeListCSV .\Samples\rangelist.csv`

Editing a discovery range group

Description: The **Set-ModifyDiscoveryRangeGroup** command allows you to edit an existing discovery range group. You can change the protocols for the discovery range group by specifying a **DiscoveryProfile.xml** file which changes the current protocol settings for the specified group. For information about the **DiscoveryProfile.xml** file, see [Creating a Discovery Profile Input File](#).

Command:

```
PS> Set-ModifyDiscoveryRangeGroup -GroupName <groupname> -Profile <DiscoveryProfile.xml> -AddRangeList <rangelist .xml or .csv file>
```

Example:

- Change a discovery range group's discovery profile and add new ranges to the discovery range group using an XML file:
`PS> Set-ModifyDiscoveryRangeGroup -GroupName WebServers-TX -Profile .\samples\snmp_only.xml -AddRangeList .\samples\new_ranges.xml`
- Change a discovery range group's discovery profile and add new ranges to the discovery range group using a CSV file:
`PS> Set-ModifyDiscoveryRangeGroup -GroupName WebServers-TX -Profile .\samples\snmp_only.xml -AddRangeListCSV .\samples\new_ranges.csv`
- Add new ranges to a discovery range group using an XML file (retaining the previously discovered profile):
`PS> Set-ModifyDiscoveryRangeGroup -GroupName WebServers-TX -AddRangeList .\samples\new_ranges.xml`
- Add new ranges to a discovery range group using a CSV file (retaining the previously discovered profile):
`PS> Set-ModifyDiscoveryRangeGroup -GroupName WebServers-TX -AddRangeListCSV .\samples\new_ranges.csv`

Removing a discovery range group

Description: The **Remove-DiscoveryRangeGroup** command allows to you to remove a discovery range group.

Command:

```
PS> Remove-DiscoveryRangeGroup -GroupName <groupname>
```

Example:

```
PS> Remove-DiscoveryRangeGroup -GroupName Group1
```

Enabling a discovery range or discovery range group

Description: The **Set-EnableDiscoveryRange** command allows you to enable a discovery range or a discovery range group. Enter the ranges either using an XML file or by specifying the range. For information about the **RangeList.xml** file, see [Specifying IPs, Ranges, or Host names Using XML or CSV Files](#).

Commands:

- `PS> Set-EnableDiscoveryRange -Range <range>`
- `PS> Set-EnableDiscoveryRange -RangeList <RangeList.xml>`
- `PS> Set-EnableDiscoveryRangeGroup -GroupName <groupname>`

Examples:

- `PS> Set-EnableDiscoveryRange -Range 10.35.1.3, 10.2.3.1`
- `PS> Set-EnableDiscoveryRange -RangeList .\Samples\RangeList.xml`
- `PS> Set-EnableDiscoveryRangeGroup -GroupName Group1`

Disabling a discovery range or discovery range group

Description: The `Set-DisableDiscoveryRange` command allows you to disable a discovery range or a discovery range group. Enter the ranges either by using an XML file or by specifying the range. For information about the `RangeList.xml` file, see [Specifying IPs, Ranges, or Host names Using XML or CSV Files](#).

Commands:

- `PS> Set-DisableDiscoveryRange -Range <range>`
- `PS> Set-DisableDiscoveryRange -RangeList <RangeList.xml>`
- `PS> Set-DisableDiscoveryRangeGroup -GroupName <groupname>`

Examples:

- `PS> Set-DisableDiscoveryRange -Range 10.35.1.3`
- `PS> Set-DisableDiscoveryRange -RangeList .\Samples\RangeList.xml`
- `PS> Set-DisableDiscoveryRangeGroup -GroupName Group1`

Creating a discovery exclude range

Description: The `Add-DiscoveryExcludeRange` command allows you to add an exclude range. Enter the ranges either by using an XML file or by specifying the range. For information about the `RangeList.xml` file, see [Specifying IPs, Ranges, or Host Names Using XML or CSV Files](#).

Commands:

- `PS> Add-DiscoveryExcludeRange -Range <range>`
- `PS> Add-DiscoveryExcludeRange -RangeList <RangeList.xml>`

Examples:

- `PS> Add-DiscoveryExcludeRange -Range 10.35.12.1`
- `PS> Add-DiscoveryExcludeRange -RangeList .\Samples\RangeList.xml`

Removing a discovery exclude range

Description: The `Remove-DiscoveryExcludeRange` command allows you to remove an exclude range. Enter the ranges either by using an XML file or by specifying the range. For information about the `RangeList.xml` file, see [Specifying IPs, Ranges, or Host Names Using XML or CSV Files](#).

Commands:

- `PS> Remove-DiscoveryExcludeRange -Range <range>`
- `PS> Remove-DiscoveryExcludeRange -RangeList <RangeList.xml>`

Examples:

- `PS> Remove-DiscoveryExcludeRange -Range 10.35.12.1`
- `PS> Remove-DiscoveryExcludeRange -RangeList .\Samples\RangeList.xml`

Running discovery, inventory, and status polling tasks

Description: The `Set-RunDiscovery`, `Set-RunInventory`, `Set-RunDiscoveryInventory`, and `Set-RunStatusPoll` commands allow you to perform discovery, inventory, and status polling on a discovery range, discovery range group, or devices. For range and range groups, enter the ranges either using an XML file or by specifying the range. For more information about the `RangeList.xml` file, see [Specifying IPs, Ranges, or Host Names Using XML or CSV Files](#). For devices, enter the name of the device as displayed in the device tree. Multiple device names must be separated by a comma.

Commands:

- `PS> Set-RunDiscovery -DeviceName <device 1>,<device 2>,...,<device N>`
- `PS> Set-RunDiscovery -Range <rangename>`
- `PS> Set-RunDiscovery -GroupName <rangeGroupName>`
- `PS> Set-RunDiscovery -RangeList <rangelist.xml>`
- `PS> Set-RunInventory -DeviceName <device 1>,<device 2>,...,<device N>`
- `PS> Set-RunInventory -Range <rangename>`
- `PS> Set-RunInventory -GroupName <rangeGroupName>`
- `PS> Set-RunInventory -RangeList <rangelist.xml>`
- `PS> Set-RunDiscoveryInventory -DeviceName <device 1>,<device 2>,...,<device N>`
- `PS> Set-RunDiscoveryInventory -Range <rangename>`
- `PS> Set-RunDiscoveryInventory -GroupName <rangeGroupName>`
- `PS> Set-RunDiscoveryInventory -RangeList <rangelist.xml>`
- `Set-RunStatusPoll -DeviceName <device 1>,<device 2>,...,<device N>`
- `PS> Set-RunStatusPoll -Range <rangename>`
- `PS> Set-RunStatusPoll -GroupName <rangeGroupName>`
- `PS> Set-RunStatusPoll -RangeList <rangelist.xml>`

Examples:

- `PS> Set-RunDiscovery -Range 10.23.23.1`
- `PS> Set-RunInventory -GroupName MyServers`
- `PS> Set-RunDiscoveryInventory -RangeList .\Samples\RangeList.xml`
- `PS> Set-RunStatusPoll -DeviceName MyZen`

Removing devices

Description: The `Remove-Device` command allows you to remove devices from the device tree.

Command:

- `PS> Remove-Device -DeviceName <device 1>,<device 2>,...,<device N>`

Example:

- `PS> Remove-Device -DeviceName Server1,RAC1`

Retrieving the status execution progress of a discovery range

Description: The `Get-DiscoveryStatus` command allows you to get the progress of a discovery range. Enter the ranges either by using an XML file or by specifying the range. For more information about the `RangeList.xml` file, see [Specifying IPs, Ranges, or Host Names Using XML or CSV Files](#).

Commands:

- PS> Get-DiscoveryStatus -Range <rangeName>
- PS> Get-Discovery -RangeList <RangeList.xml>
- PS> Get-Discovery -GroupName <group name>

Examples:

- PS> Get-DiscoveryStatus -Range 10.35.2.1
- PS> Get-Discovery -RangeList .\Samples\RangeList.xml
- PS> Get-Discovery -GroupName Group1

Stopping discovery range or group tasks

Description: For any range, only one type of task, such as discovery, discovery and inventory, or status polling, can run at a given time. The Set-StopTask command allows you to stop a task associated with a discovery range or the tasks associated with the ranges belonging to a discovery range group.

Commands:


- PS> Set-StopTask -Range <rangename>
- PS> Set-StopTask -GroupName <groupname>

Examples:

- PS> Set-StopTask -Range 10.35.1.12
- PS> Set-StopTask -GroupName Group1

Creating a custom device group

Description: The Add-CustomGroup command allows you to create a custom device group in the device tree. If required, you can add devices to the group after it is created.

 **NOTE:** By using OpenManage Essentials CLI, you can only create static groups which contain a finite list of servers. You can create dynamic groups based on queries by using the OpenManage Essentials console. For more information, see [Creating a New Group](#).

Commands:

- PS> Add-CustomGroup -GroupName <groupName>
- PS> Add-CustomGroup -GroupName <groupName> -DeviceList <DeviceList.xml>
- PS> Add-CustomGroup -GroupName <groupName> -Devices <comma separated list of devices>

Examples:

- PS> Add-CustomGroup -GroupName MyServers -DeviceList .\Samples\devicelist.xml
- PS> Add-CustomGroup -GroupName MyServers -Devices PE2900-WK28-ZMD, PWR-CODE.US.DELL.COM, HYPERVISOR, M80504-W2K8

Example of a DeviceList.xml file:

```
<DeviceList>
  <Device Name="PE2900-WK28-ZMD"/>
  <Device Name="PWR-CODE.US.DELL.COM"/>
  <Device Name="HYPERVISOR"/>
  <Device Name="M80504-W2K8"/>
</DeviceList>
```

Adding devices to a custom group

Description: The Add-DevicesToCustomGroup command allows you to add devices to an existing group. To add the devices to the group, either use an XML file or list the devices and separate them using a comma.

Commands:

- `PS> Add-DevicesToCustomGroup -GroupName <groupName> -DeviceList <devicelist.xml>`
- `PS> Add-DevicesToCustomGroup -GroupName <groupName> -Devices <comma separated list of devices>`

Examples:

```
PS> Add-DevicesToCustomGroup -GroupName MyServers -DeviceList .\Samples\DeviceList.xml
```

or

```
PS> Add-DevicesToCustomGroup -GroupName MyServers -Devices PE2900-WK28-ZMD, PWR-CODE.US.DELL.COM, HYPERVISOR, M80504-W2K8
```

Example of a DeviceList.xml file:

```
<DeviceList>
  <Device Name="PE2900-WK28-ZMD"/>
  <Device Name="PWR-CODE.US.DELL.COM"/>
  <Device Name="HYPERVISOR"/>
  <Device Name="M80504-W2K8"/>
</DeviceList>
```

Deleting a custom device group

Description: The `Remove-CustomGroup` command allows you to remove a group from the root node.

Command:

```
PS> Remove-CustomGroup -GroupName <groupName>
```

Example:

```
PS> Remove-CustomGroup -GroupName MyServers
```