Dell EMC OpenManage Integration Version 7.3 with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM)

Security Configuration Guide

July 2021
Rev. A00

DELL EMC

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

Figures

Tables

1

PREFACE

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document. This document was accurate at publication time. To ensure that you are using the latest version of this document, go to https://www.dell.com/support.

Legal disclaimers

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANT ABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL DELL TECHNOLOGIES, ITS AFFILIATES OR SUPPLIERS, BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING FROM OR RELATED TO THE INFORMATION CONTAINED HEREIN OR ACTIONS THAT YOU DECIDE TO TAKE BASED THERE ON, INCLUDING ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF DELL TECHNOLOGIES, ITS AFFILIATES OR SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Dell Technologies takes reports of potential security vulnerabilities in our products very seriously. If you discover a security vulnerability, you are encouraged to report it to Dell immediately. Dell Technologies distributes Security Advisories to bring important security information to the attention of users of the impacted product(s). Dell Technologies assesses risk based on an average of risks across a diverse set of installed systems and may not represent the actual risk to your local installation and individual environment. It is recommended that all users determine the applicability of this information to their individual environments and take appropriate actions. All aspects of Dell's Vulnerability Response Policy are subject to change without notice and on a case-by-case basis. Your use of the information contained in this document or materials linked here in is at your own risk. Dell reserves the right to change or update this document in its sole discretion and without notice at any time.

Purpose

This document includes information about security features and capabilities of Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM).

- Understand the accessibility and data security of the OMIMSSC for SCOM product.
- Know how to follow the recommendation or best practices of the appliance to maximize the security posture in your environment.
- Understand the expectations to be fulfilled from security aspects for deploying OMIMSSC for SCOM.

Audience

This document is intended for system administrators who are responsible for managing security for OMIMSSC for SCOM.

Revision History

The following table presents the revision history of this document.

Table 1. Revision History

Revision	Date	Description
A00	July 2021	Initial release of the OMIMSSC version 7.3 for SCOM Security Configuration Guide.

Related documentation

In addition to this guide, you can access the other guides available at https://www.dell.com/support. Click **Browse all products**, then click **Software** > **Enterprise Systems Management**. Click **OpenManage Integration for Microsoft System Center Operations Manager (SCOM)** and select **OpenManage Integration for Microsoft System Center Operations Manager (SCOM) 7.3** to access the following documents:

- *Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) User's Guide*
- *Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) Release Notes*

You can find the technical artifacts including technical white papers at https://www.dell.com/support.

Reporting security vulnerabilities

Dell EMC takes reports of potential security vulnerabilities in our products very seriously. If you discover a security vulnerability, you are encouraged to report it to Dell EMC immediately.

For the latest on how to report a security issue to Dell, see the Dell Vulnerability Response Policy on the Dell.com site.

2

Security Quick Reference

Topics:

Deployment models

You can deploy Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (OMIMSSC) as a VHD or OVA in Hyper-V or ESXi environment, as applicable.

Virtual Hard Disk (VHD) and Open Virtual Appliance (OVA) deployment

OMIMSSC is available in VHD and OVA formats. It can be downloaded online. Go to https://www.dell.com/support and select **Browse all products > Software > Enterprise Systems Management > OpenManage Integration for Microsoft System Center Operations Manager (SCOM)**. Select the required OMIMSSC version and download the VHD or OVA file. Deploy the OMIMSSC Appliance on Hyper-V or ESXi as a virtual machine, as applicable.

The VHD and OVA deployment models include a pre-configured bundle with the OMIMSSC software and the Linux operating system that the OMIMSSC software runs on.

The VHD and OVA environment also includes a pre-configured firewall that is tuned to the OMIMSSC communication requirement with the integrated systems.

For more information about deploying OMIMSSC, see the *Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) User`s Guide* available at https://www.dell.com/support.

Security profiles

OMIMSSC for SCOM by default installs and configures the self-signed certificate for the management website. To avoid potential security risks, recommendation is to use a trusted certificate signed by a Certificate Authority (CA). It is highly recommended to replace the Certificate Authority (CA) signed certificates for the stronger security environments.

3

Product and Subsystem Security

Topics:

Security Controls Map

The OMIMSSC appliance for SCOM performs discovery and monitoring of PowerEdge servers, chassis, and network switches on the SCOM console. iDRAC can communicate with appliance over HTTPS and NFS for different system related updates.

The User Interface of OMIMSSC for SCOM is the OMIMSSC Admin Portal. The Dell EMC OpenManage Integration Dashboard operates from the SCOM console and provides host hardware management capabilities.

Credentials to access managed nodes and SCOM console are stored in an encrypted format in the database. OMIMSSC appliance interacts over PowerShell with SCOM for synchronizing information.

The following figure displays the OMIMSSC for SCOM security controls map.

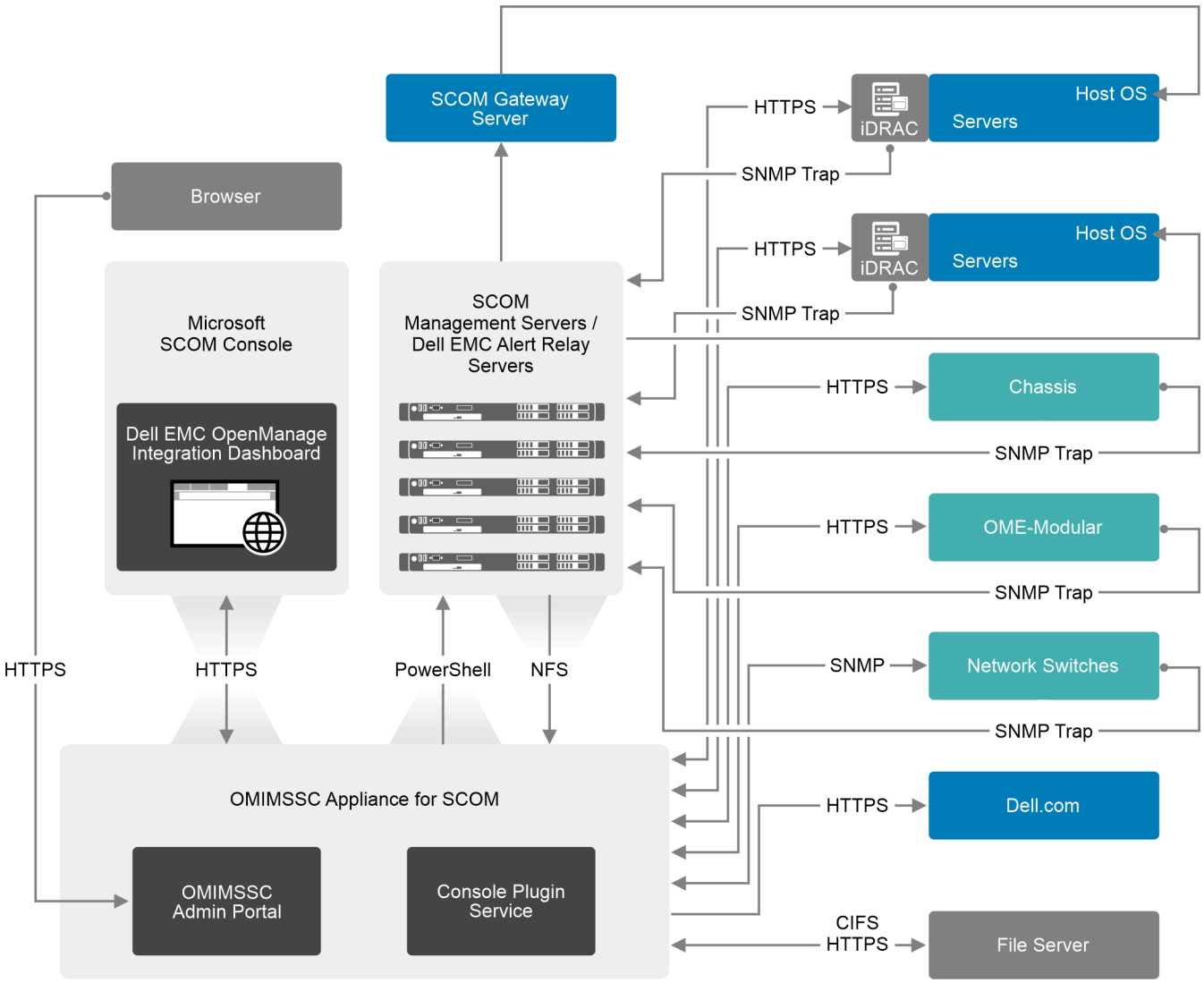

Figure 1. OMIMSSC for SCOM security controls map

Authentication

Access control

Access control settings provide protection of resources against unauthorized access. Dell EMC OpenManage Integration Dashboard accessed by Microsoft System Center Operations Manager (SCOM) console provide users with appropriate roles and privileges configured in Microsoft Active Directory. OMIMSSC Admin Portal access is given to OMIMSSC appliance admin account.

For more information on roles and privileges, see User and credential management on page 16.

OMIMSSC Appliance administration

Default user accounts

OMIMSSC for SCOM includes the following default user accounts:

- Local user account (Admin account)
- Read-only user account
- Root account

Local user account (Admin account)

OMIMSSC for SCOM provides a single default local administrative user account. The username of this internal account is *admin*. The local administrator has access to all operations in the Dell EMC OMIMSSC Admin Portal only. The first time that you deploy OMIMSSC, you are prompted to set the password. Follow the on-screen instruction to set the password.

Read-only user account

OMIMSSC for SCOM provides a single default local read-only user account. The username of the read-only account is *readonly*.

The user with read-only permissions can log in to OMIMSSC for SCOM using the VM remote console only.

This account can be used during troubleshooting to view critical appliance status and logs.

Root account

OMIMSSC for SCOM appliance has Operating System root account.

This default account is not accessible. Technical support team will require root account to debug the field issues.

For more information about roles and privileges, see User and credential management on page 16.

Infrastructure monitoring using Microsoft System Center Operations Manager (SCOM) Console

SCOM Console user accounts

OMIMSSC depends on authentication, authorization, and security policies provided by the Microsoft Active Directory. Microsoft System Center Console users can access the Dell EMC OpenManage Integration Dashboard when the console users have appropriate roles and privileges on Microsoft Active Directory.

OMIMSSC provide integration with following Microsoft System Center Console.

Microsoft System Center Operations Manager (SCOM) console

SCOM console allows you to manage roles and permissions as follows. Dell EMC OpenManage Integration Dashboard on the SCOM console is used to interact with the OMIMSSC appliance.

Role-based security:

In the SCOM console, user roles are required to access the data of monitored devices and perform various tasks. User roles are applied to groups of users who need access to perform tasks on the monitored devices. By default, only the Operations Manager Administrator account has the required privileges to access and act on the monitored data. Other users must be assigned a user role to view or act on all monitored data or specific data.

Roles specify what users can do in the SCOM console. Roles consist of a profile that defines a set of available operations for the role, scope which define the set of objects on which the role can operate, and a membership list that defines the Active Directory user accounts and security groups that are assigned to the role.

For more information about roles and privileges in Microsoft System Center Operations Manager, go to https://docs.microsoft.com/en-us/system-center/scom/manage-security-overview?view=sc-om-2019.

Login security settings

OMIMSSC Appliance administration

OMIMSSC console uses local user account (admin account) to access OMIMSSC Admin Portal and virtual appliance. It validates the user authentication on appliance. Admin account has logout option post administration operations are completed. On OMIMSSC Admin Portal, web session is maintained for maximum 15 minutes and a maximum of 200 concurrent sessions are

allowed at any given time. OMIMSSC admin account supports multiple account logins and each account login has a separate session

Failed login behavior

OMIMSSC for SCOM includes security settings when there are multiple unsuccessful authentication occurrences. For invalid login attempts the user is prompted with the `User Name or Password is incorrect` message.

Local user account lockout

After three consecutive failed attempts to login to the local user account, OMIMSSC for SCOM temporarily locks out the user for a period of one minute.

Automatic session timeout

By default, after 15 minutes of inactivity, the OMIMSSC session times out and you are automatically logged out.

Infrastructure monitoring using Microsoft System Center Operations Manager (SCOM) Console

Failed login behavior

OMIMSSC leverages Microsoft Active Directory to verify the authentication and authorization of the user. Dell EMC OpenManage Integration Dashboard login page shows appropriate error message for unsuccessful authentication occurrences. For invalid login attempts the user is prompted with the message: `Unable to log in. Ensure that correct credentials are entered and confirm that account is not locked in Active Directory. The login will also fail is a de-enrollment job is in progress.`

Microsoft System Center Console user account lockout

OMIMSSC leverages Microsoft Active Directory to verify the validity of the user. Account lockout policies configured in Active Directory temporarily locks out the user for a set period as defined by lockout policies. Dell EMC OpenManage Integration Dashboard login page shows appropriate error message when there are unsuccessful authentication occurrences due to account lockout.

For more information about roles and privileges, see https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/ad-fs-password-protection

Automatic session timeout

The session timeout is applicable for session created with Dell EMC OpenManage Integration Dashboard user. By default, after 15 minutes of inactivity, the Dell EMC OpenManage Integration Dashboard session times out and you are automatically logged out. For more information about roles and privileges, see User and credential management on page 16.

Authentication types and setup considerations

OMIMSSC Appliance administration

Authentication types

OMIMSSC for SCOM supports basic username and password-based authentication. OMIMSSC appliance credentials are stored in appliance in secured manner. Admin user can log in to OMIMSSC Admin Portal and appliance VM console using valid credentials.

Setup considerations

OMIMSSC admin operations for setup

OMIMSSC admin performs the following operations to integrate with Microsoft System Center Operations Manager (SCOM) Console.

Download Dell EMC Alert Relay Server Installer

1. Log in to the OMIMSSC admin portal by using admin user and password.

   Admin Portal URL: https://<IP address or FQDN>

2. Click **Downloads** and click **Dell EMC Alert Relay Server Installer** to download the installer.

   For more information about downloading and installing the Dell EMC Alert Relay Server Installer, see *Scalability with Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) technical white paper* available at https://www.dell.com/support

Enroll SCOM Management Group and Dell EMC Alert Relay Servers with OMIMSSC appliance

1. Log in to the OMIMSSC admin portal by using admin user and password.

   Admin Portal URL: https://<IP address or FQDN>

2. Click **Settings** and click **Console Enrollment** to enroll SCOM Management Group and Dell EMC Alert Relay Servers with OMIMSSC appliance.

   For more information, see *Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) User`s Guide* available at https://www.dell.com/support.

OMIMSSC appliance uses Windows PowerShell Remoting to run PowerShell commands on Microsoft System Center Operations Manager (SCOM) Console. Enrollment process uses PowerShell cmdlet internally to authenticate and authorize Microsoft System Center user. It creates application profile on respective SCOM console to provide the launch point for Dell EMC OpenManage Integration Dashboard. For more information on PowerShell remoting, see Windows PowerShell Remoting on page 15.

Infrastructure monitoring using Microsoft System Center Operations Manager (SCOM) Console

Authentication types

Dell EMC OpenManage Integration Dashboard supports basic username and password-based authentication. Microsoft System Center Console account credentials are stored on Microsoft Active Directory. Credentials which are required to communicate with SCOM Management Servers and Dell EMC Alert Relay Servers from appliance are created through credential profile and stored on OMIMSSC appliance.

Setup considerations

Dell EMC OpenManage Integration Dashboard operations for setup

Dell EMC OpenManage Integration Dashboard provides interface in SCOM console. To access Dell EMC OpenManage Integration Dashboard, OMIMSSC appliance provide login page for the SCOM Console Users.

OMIMSSC appliance depends on Microsoft Active Directory (AD) for user authentication to access OpenManage Integration Dashboard pages. It validates the user authentication on AD on periodic basis. It maintains the session for 30 minutes in OMIMSSC before re-validating the user with AD.

Launch Dell EMC OpenManage Integration Dashboard

SCOM Console user must have the Microsoft System Center access and privilege to launch the Dell EMC OpenManage Integration Dashboard. For more information about launching and using Dell EMC OpenManage Integration Dashboard, see the *Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) User`s Guide* available at https://www.dell.com/support.

Access OMIMSSC appliance from enrolled SCOM console

Security roles and permissions

The Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) stores admin account credentials in an encrypted format. It does not provide these credentials to client applications to avoid any improper requests. The backup database is fully encrypted by using custom security phrases, and hence data cannot be misused.

The backup database is fully encrypted by using GNU Privacy Guard (GPG). The backup data is stored in a CIFS share provided by the authorized user. This CIFS share can be accessed by authorized users only. Backup operation expect users to provide password for additional protection. The backup password provided by user is not stored in the appliance, hence users have to remember it and provide the same password during restore operation.

For Microsoft System Center User account, user with full administrator role in the Microsoft Active Directory administrators group have all the privileges in OMIMSSC. This user can use all the functions of the Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM).

Data integrity

The communication between the OMIMSSC appliance and Microsoft System Center Operations Manager (SCOM), SCOM Management Servers, and Dell EMC Alert Relay Servers is accomplished by PowerShell Remoting.

A secure PowerShell remote session will be created post user authentication and the applicable PowerShell scripts will be executed using this remote session. For more information, see Windows PowerShell Remoting on page 15.

The communication between SCOM and OMIMSSC appliance is over HTTPS. The OMIMSSC appliance generates a certificate that is used for trusted communication between SCOM and the appliance.

Access control authentication, authorization, and roles

To perform operations on managed nodes by Microsoft System Center Operations Manager (SCOM) Console, OMIMSSC uses the current user session and authorization available in Microsoft System Center console.

Windows PowerShell Remoting

Using the WS-Management protocol, Windows PowerShell Remoting lets you run any Windows PowerShell command on one or more SCOM Management Servers and Dell EMC Alert Relay Servers. You can establish persistent connections, start interactive sessions, and run scripts on remote computers.

To use Windows PowerShell Remoting, the remote computer must be configured for remote management.
For more information, including instructions, see https://docs.microsoft.com/EN-US/POWERSHELL/MODULE/MICROSOFT.POWERSHELL.CORE/ABOUT/ABOUT_REMOTE_REQUIREMENTS?VIEW=POWERSHELL-7.

To enable PowerShell Remoting, see PowerShell Permission on page 24.

User and credential management

OMIMSSC Appliance administration

OMIMSSC appliance comes with default pre-loaded accounts and does not support custom accounts.

Pre-loaded accounts

The following table describes the pre-loaded OMIMSSC accounts:

Table 2. Pre-loaded accounts and default credentials

User Account	Username	Password	Description
Admin User	admin	Set on first boot after deployment. For more information about changing admin password, see Change OMIMSSC appliance admin password on page 16.	The default user for OMIMSSC web application administration and OMIMSSC Appliance VM console.
Read-only user	readonly	Set on first boot after deployment. The readonly user password can be reconfigured after logging in as readonly user using standard Linux password change commands.	OMIMSSC provides a single default local read only user account. The administrator can log into OMIMSSC using the VM remote console only. This account can be used during troubleshooting to view critical appliance status and logs.
Linux operating system root	root	The OS root password is set when OMIMSSC is deployed.	The root operation system account is not accessible. Technical support team uses root account to debug the field issues.

Managing credentials

If you are logging in for the first time to Dell EMC OMIMSSC Admin Portal, log in as an administrator (the default username is **admin**).

NOTE: If you forget the administrator password, it cannot be recovered from the OMIMSSC appliance.

Change OMIMSSC appliance admin password

About this task

About this task

You can change the OMIMSSC appliance password in the OMIMSSC Appliance VM console.

Steps

To change the password of OMIMSSC Appliance VM console, perform the following steps:

Steps

1. Launch OMIMSSC Appliance VM console, and login using the old credentials.
2. Navigate to **Change Admin Password** and click **Enter**.
   The screen to change password is displayed.
3. Provide your present password, and then provide a new password matching the listed criteria. Re-enter the new password and click **Enter**.
   The status after changing the password is displayed.
4. To come back to home page, click **Enter**.

   NOTE: Appliance will reboot after changing the password.

Infrastructure monitoring using Microsoft System Center Operations Manager (SCOM) Console

Microsoft System Center Operations Manager (SCOM) Console users can access the Dell EMC OpenManage Integration Dashboard when the users have appropriate roles and privileges on Microsoft Active Directory.

OMIMSSC uses predefined users in Microsoft Active Directory. OMIMSSC maintains the credential profiles to access Microsoft System Center consoles. Each profile is mapped to single user in Microsoft Active Directory. For more information about credential profile management, see Credential profiles to access Microsoft System Center Operations Manager (SCOM) Console on page 17.

Credential profiles to access Microsoft System Center Operations Manager (SCOM) Console

Credential profiles simplify the use and management of user credentials by authenticating the role-based capabilities of the user. Each credential profile contains a username and password for a single user account. OMIMSSC uses credential profiles to connect to the managed system's iDRAC. Also, you can use credential profiles to access resources available in Windows shares and to work with different features of iDRAC.

You can create the following credential profiles:

- Device Credential Profile-used to log in to iDRAC or CMC. Also, you can use this profile to discover a server, chassis, and network switches, resolve synchronization issues, and deploy operating system. This profile is specific to a console. You can use and manage this profile only in a console where it is created.
- Windows Credential Profile-used for enrolling SCOM Management Group with the OMIMSSC appliance and for accessing share folders in Windows operating system.

NOTE: All profiles other than device profile are shared resources. You can use and manage these profiles from any of the enrolled consoles.

Authorization

OMIMSSC Appliance administration

OMIMSSC Appliance Admin Account Privileges

OMIMSSC appliance supports an admin user account.

After logging in to OMIMSSC, administrator can access only the OMIMSSC appliance configuration features such as:

- Import valid license
- Upgrade OMIMSSC appliance using service packs and backup and restore
- Restore OMIMSSC Appliance
- Backup OMIMSSC Appliance
- Generate a Certificate Signing Request (CSR)
- Upload HTTPS certificate

- Enrolled SCOM consoles
- Generate and download the troubleshooting bundle
- For invalid login attempts the user prompted with `User Name or Password is incorrect` message.

Infrastructure monitoring using Microsoft System Center Operations Manager (SCOM) Console

Microsoft System Center user account privileges

All the required account privileges to use OMIMSSC are as follows:

User must be member of the following groups in System Center Consoles for Account privileges to use Dell EMC OpenManage Integration Dashboard.

Table 3. User accounts with required privileges

Users	Privileges/Roles
For enrollment	• Account used to enroll SCOM Management Group with the OMIMSSC appliance should be a local admin on the SCOM Management Server and must have Operations Manager administrative role. • Domain user. • Member of Local Administrator group in system center machine.
For logging in to Dell EMC OpenManage Integration Dashboard	• Domain user. • Member of Local Administrator group in system center machine. • Member of Operations Manager administrative role.

Network security

OMIMSSC appliance uses a preconfigured firewall to enhance security by restricting inbound and outbound network traffic to the TCP and UDP ports. The tables in this section lists the inbound and outbound ports that OMIMSSC uses.

Network exposure

Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) uses inbound and outbound ports when communicating with remote systems.

Port information and communication matrix for OMIMSSC appliance

To connect the OMIMSSC appliance with the applications and devices that must be monitored by OMIMSSC, you must ensure that certain ports, protocols, and communication networks are available and enabled on OMIMSSC and the SCOM Management Servers.

Table 4. Port information for OMIMSSC appliance

Communication purpose	Port number	Protocols	Direction	Source	Destination	Description
HTTP Server	80	TCP	In	OMIMSSC Admin Portal	OMIMSSC appliance	Used for redirection from HTTP to HTTPS while loading OMIMSSC Admin Portal.

Table 4. Port information for OMIMSSC appliance (continued)

Communication purpose	Port number	Protocols	Direction	Source	Destination	Description
Inventory or health update to SCOM	111	TCP	In	SCOM management server	OMIMSSC appliance	Appliance permits NFS share to share the inventory details to management packs.
UI operations from the SCOM view	443	TCP	In	SCOM management server	OMIMSSC appliance	UI operations using OMIMSSC dashboard which is started from the SCOM console.
NFS Share	2049	TCP/ UDP	In	SCOM management server	NFS	NFS share that is used by OMIMSSC appliance to the managed nodes and systems that are used in enrollment and device health monitoring flow.
NFS Share	4003	TCP/ UDP	In	SCOM management server	OMIMSSC appliance	Used for mountd service.
DNS Client	53	TCP	Out	OMIMSSC appliance	DNS Server	Connectivity to DNS Server for resolving the host names.
Dynamic network configuration	67 and 68	UDP	Out	OMIMSSC appliance	DHCP Server	To get network details such as IP, Gateway, Netmask, DNS, and DHCP.
Internet	80	TCP	Out	OMIMSSC appliance	Dell Online Data Access	To connect to the Service Pack Update repository of OMIMSSC appliance for SCOM.
SNMP	161	UDP	Out	OMIMSSC appliance	Managed Nodes (iDRAC, CMC, or network devices)	To connect to the Managed Node for collecting inventory and health information.
HTTPS Server	443	TCP	Out	OMIMSSC appliance	Managed Nodes (iDRAC, CMC, or network devices)	Uses WS-Man, Redfish, or SNMP.
Windows Network Share	445/139	SMB	Out	OMIMSSC appliance	Windows Network Share	Used to back up and restore files of OMIMSSC appliance settings and data
PowerShell Connectivity between Appliance and Managed System Host OS	5985 and 5986	TCP	Out	OMIMSSC Appliance	SCOM Management Server	Windows event is created using Remote PowerShell. Dell EMC Management Pack Rules monitor the events and updates the SCOM DB.

Table 5. Port information for SCOM Management Servers and Dell EMC Alert Relay Servers

Communication purpose	Port number	Protocols	Direction	Source	Destination	Description
SNMP traps	162	UDP	In	iDRAC, CMC, network devices	All SCOM Management Servers and Dell EMC Alert Relay Servers	OMIMSSC distributes the total devices to all the Alert Relay Servers. Alert Relay Servers receive the alert and converts to Windows events.

Table 5. Port information for SCOM Management Servers and Dell EMC Alert Relay Servers (continued)

Communication purpose	Port number	Protocols	Direction	Source	Destination	Description
Health or metrics update to SCOM	5985 and 5986	TCP	In	OMIMSSC appliance	All SCOM Management Servers	PowerShell commands are started from the appliance.
Inventory or health update to SCOM	111 and 2049	TCP and UDP	Out	All SCOM Management Servers	OMIMSSC appliance	Appliance permits NFS share to share the inventory details with management packs.
UI operations	443	TCP	Out	All SCOM Management Servers	OMIMSSC appliance	UI operations using OMIMSSC dashboard which is started from the SCOM console.

Table 6. Port information for Dell EMC devices (iDRAC, CMC, OME-Modular, or network switch)

Communication purpose	Port number	Protocols	Direction	Source	Destination	Description
SNMP traps	162	UDP	Out	iDRAC, CMC, or network devices	All SCOM Management Servers and Dell EMC Alert Relay Servers	OMIMSSC distributes the total devices to all Alert Relay Servers. Alert Relay Servers receive the alert and converts to Windows events.
Health, metrics, or inventory collection from devices	443	TCP	In	OMIMSSC Appliance	iDRAC, CMC, or network devices	Uses WS-Man, Redfish, or SNMP.

Data security

The data that is maintained by OMIMSSC is stored and secured in internal databases within the appliance and it cannot be accessed from outside. OMIMSSC uses AES-256 based encryption for data security.

The data in transit is protected using HTTPS protocol.

Data at rest encryption

This section describes the capabilities for data-at-rest encryption in OMIMSSC. The sensitive data is stored in encrypted format in the database. AES encryption algorithm is used with 256 key size.

OMIMSSC has encryption key management in place as described below.

Generate Encryption Key

OMIMSSC supports appliance unique encryption key. Each appliance generates a new key during appliance boot up sequence. Access controls are in place to protect encryption key, key-store, and password.

Change Encryption Key

Encryption key can be changed by changing the password for admin account. Similarly, new encryption key will be used when appliance is restored from one version to a higher version.

For more information, see Change OMIMSSC appliance admin password on page 16.

Sensitive Data Migration

While migrating from old appliance, the old data will be stored as backup file, the key-store and password will be exported as part of backup procedure. While restoring the data on new appliance, the sensitive data will be re-encrypted using new encryption key. For additional security, admin user provides password to protect the exported backup files.

Following are the steps to migrate data:

1. Backup the OMIMSSC appliance data using Admin portal. Backup data will be stored on CIFS share. CIFS share can be accessed by authorized personnel only.
2. Restore the data on the new OMIMSSC appliance.

Cryptography

OMIMSSC uses cryptography for the following components:

- Access control
- Authentication
- Digital signatures

Manage HTTPS certificate

OMIMSSC uses x.509 PKI standard based certificates for secure HTTP access (HTTPS).

By default, OMIMSSC installs and uses the self-signed certificate for the HTTPS secure transactions.

For stronger security, it is recommended to use the Certificate Authority (CA) or Enterprise CA signed certificates.

The self-signed certificate is sufficient to establish an encrypted channel between web browsers and the server. The self-signed certificate cannot be used for authentication.

You can use the following types of certificates for OMIMSSC authentication:

- A self-signed certificate

  OMIMSSC generates self-signed certificates when the hostname of the appliance is configured.

- A certificate that is signed by a trusted certificate authority (CA) vendor.

Update certificates for registered OMIMSSC servers

About this task

The OMIMSSC uses OpenSSL API to create the Certificate Signing Request (CSR) by using the RSA encryption standard with a 2048-bit key length.

The CSR generated by OMIMSSC gets a digitally signed certificate from a trusted certification authority (CA). The OMIMSSC uses the digital certificate to enable HTTPS on the web server for secure communication. You can upload CA signed certificate using admin portal.

For more information about HTTPS certificate management in OMIMSSC, see *Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) User's Guide* available at https://www.dell.com/support.

Auditing and logging

Appliance logs

Appliance logs display all OMIMSSC Appliance-specific log messages such as restarting OMIMSSC appliance. You can view this category of messages only from OMIMSSC Admin Portal.

For more information on specific logs and filters, see *Jobs and Log Center* section in OMIMSSC for SCOM User's Guide.

Web server logs

The admin user can use the OMIMSSC administration console to generate a troubleshooting bundle with all the relevant logs.

For more information, see Download troubleshooting bundle .

The read-only account helps troubleshoot the appliance by allowing the user to read various parameters of the appliance at runtime. For advanced troubleshooting, see the Tech support guides to check specific parameters.

Download troubleshooting bundle

Prerequisites

To generate the troubleshooting bundle, ensure that you log in to the OMIMSSC Admin Portal.

About this task

The troubleshooting bundle contains OMIMSSC appliance logging information that can be used to help in resolving issues or sent to Technical Support. OMIMSSC does not log any user sensitive data.

NOTE: The downloaded troubleshooting bundle will not carry logs collected from SCOM Management Servers and Dell EMC Alert Relay Servers.

Steps

1. On the **OMIMSSC Admin Portal**, click **Settings** > **Logs**.
   The **Troubleshooting Bundle** dialog box is displayed.
2. In the **Troubleshooting Bundle** dialog box, click **Download Troubleshooting Bundle**.
   Depending on the size of the logs, creating the bundle may take some time.

Results

Automatic file download will start. The **Troubleshooting Bundle** file will be available in download folder as per browser configuration.

Serviceability

The support website https://www.dell.com/support provides access to licensing information, product documentation, advisories, downloads, and troubleshooting information. This information helps you to resolve a product issue before you contact support team.

Special permission is required to login to OMIMSSC for service personnel. If the troubleshooting bundle is not sufficient, the personnel can enable the root user to collect more information.

Ensure that you install security patches and other updates when they are available, including the OMIMSSC Operating System update.

Security patches

Periodic OMIMSSC updates that include security updates, and security only updates released as required.

The updates are cumulative and published on the Dell Technologies support site. OMIMSSC users receive recommendations to install or update the OMIMSSC Appliance on the **Updates and Recommendations** page on the native Microsoft SCOM console.

OMIMSSC Operating System update

Periodically, security patches and fixes are released for the OMIMSSC Operating System.

These fixes must be installed on existing VHD and OVA deployments of OMIMSSC through service packs. When available, it is highly recommended that you install these security patches and fixes on the OMIMSSC server through service packs.

Product code integrity

The OMIMSSC software installer is signed by Dell. Download installation software from https://www.downloads.dell.com. To ensure the integrity of your download, verify the checksum value. Checksums are available in MD5, SHA1, and SHA-256. It is recommended that you verify the authenticity of the OMIMSSC installer signature.

In PowerShell, `Get-FileHash` cmdlet can compute the hash value for the OMIMSSC_<version>_<build>_SCOM.<vhd or ova>_<revision>.zip file. The hash algorithm used is the default SHA-256. Then, you can compare the hashes to validate integrity. For more details to generate hash for file, see https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-7.1&viewFallbackFrom=powershell-6.0

4

Miscellaneous Configuration and Management

Topics:

Licensing of Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM)

OMIMSSC has two types of licenses:

- Evaluation license—this is a trial version of the license containing an evaluation license for five servers (hosts or unassigned) which is auto imported after the installation. This is applicable only for 11th and later generations of Dell EMC PowerEdge servers.
- Production license—you can purchase production license from Dell EMC for any number of servers to be managed by OMIMSSC. This license includes product support and OMIMSSC Appliance updates.

When you purchase a license, the XML file (license key) is available for download through the Dell Digital Locker. If you are unable to download your license key(s), contact Dell Support by going to https://www.dell.com/support/softwarecontacts to locate the regional Dell Support phone number for your product.

You can discover servers in OMIMSSC using a single license file. If a server is discovered in OMIMSSC, a license is used. And, if a server is deleted, a license is released. An entry is made in the activity log of OMIMSSC for the following activities:

- License file is imported.
- Server is deleted from OMIMSSC, and license is relinquished.
- License is consumed after discovering a server.

After you upgrade from an evaluation license to a production license, the evaluation license is overwritten with the production license. The **Licensed Nodes** count is equal to the number of production licenses purchased.

Manage backup and restore in OMIMSSC

To protect the OMIMSSC appliance for SCOM from a disaster scenario, it is recommended that you perform backups of OMIMSSC. If required, you can restore OMIMSSC settings and data from these backups. For more information about backup and restore, see *Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) User's Guide* available at https://www.dell.com/support.

PowerShell Permission

Check if the PSRemoting status is enabled and ExecutionPolicy is set to RemoteSigned on the SCOM Management Servers and Dell EMC Alert Relay Servers. If the status is different, perform the following actions:

- In PowerShell run the command: `PSRemoting`.

  If the PSRemoting command is disabled, enable the PSRemoting command using the following commands.

- Run the command: `Enable-PSRemoting`.
- In the confirmation message, enter **`Y`**.

- In PowerShell, run the command: `Get-ExecutionPolicy`.

  If the policy is not set to RemoteSigned, set it to RemoteSigned by using the following commands.
  - Run the command: `Set-ExecutionPolicy RemoteSigned`.
  - In the confirmation message, enter **`Y`**.