

OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager Security Configuration 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.

Tables.....	5
Chapter 1: PREFACE.....	6
Chapter 2: Security Quick Reference.....	8
Deployment models.....	8
Virtual Hard Disk (VHD) and Open Virtual Appliance (OVA)deployment.....	8
Security profiles.....	8
Chapter 3: Product and Subsystem Security.....	9
Security Controls Map.....	9
Authentication.....	10
Access control.....	10
OMIMSSC Appliance administration.....	10
Infrastructure administration using Microsoft System Center Console	11
Login security settings.....	11
Failed login behavior.....	12
Local user account lockout.....	12
Automatic session timeout.....	12
Infrastructure administration using Microsoft System Center Console.....	12
Authentication types and setup considerations.....	12
OMIMSSC Appliance administration.....	12
Infrastructure administration using Microsoft System Center Console	13
User and credential management.....	15
Pre-loaded accounts.....	15
Managing credentials.....	15
Authorization.....	16
Infrastructure administration using Microsoft System Center Console	17
Network security.....	17
Network exposure.....	17
Management Station Ports.....	17
Data security.....	19
Data at rest encryption.....	19
Generate Encryption Key.....	19
Change Encryption Key.....	19
Sensitive Data Migration.....	20
Cryptography.....	20
Manage HTTPS certificate	20
Auditing and logging.....	21
Download troubleshooting bundle.....	21
Serviceability.....	21
Security patches.....	21
OMIMSSC Operating System update.....	22
Product code integrity.....	22

Chapter 4: Miscellaneous Configuration and Management.....23

OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint
Configuration Manager and System Center Virtual Machine Manager (OMIMSSC) licensing 23

Manage backup and restore in OMIMSSC.....23

PowerShell Permission.....23

Configuring user access to WMI for MECM.....24

1	Revision History.....	7
2	Pre-loaded accounts and default credentials.....	15
3	User accounts with required privileges.....	17
4	Ports OMIMSSC uses for listening.....	17
5	Ports OMIMSSC uses as client.....	18

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 OpenManage Integration for Microsoft System Center (OMIMSSC) 7.3 for Microsoft Endpoint Configuration Manager (MECM) and System Center Virtual Machine Manager (SCVMM).

NOTE: Microsoft Endpoint Configuration Manager (MECM) was earlier known as System Center Configuration Manager (SCCM).

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

Audience

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

Revision History

The following table presents the revision history of this document.

Table 1. Revision History

Revision	Date	Description
A00	June 2021	Initial release of the OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager 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 Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager** to access the following documents:

- *OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager Version 7.3 User's Guide* *OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager Version 7.3 Release Notes*

You can find the technical artifacts including 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.

Security Quick Reference

Topics:

- Deployment models
- Virtual Hard Disk (VHD) and Open Virtual Appliance (OVA) deployment
- Security profiles

Deployment models

You can deploy OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager (OMIMSSC) as an VHD and OVA in Hyper V and ESXi environment as applicable.

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

OMIMSSC available in VHD and OVA formats. It can be downloaded online. Visit <https://www.dell.com/support> and proceed with **Browse all products > Software > Enterprise Systems Management > OpenManage Integration for Microsoft System**. Select the required OMIMSSC version. Deploy the OMIMSSC Appliance on a Hyper-V and ESXi as a virtual machine as applicable.

The VHD and OVA deployment model includes 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 *OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager 7.3 User's Guide* available at <https://www.dell.com/support>.

Security profiles

OMIMSSC by default installs and configures the self-signed certificate for the management website. To avoid potential security risks, recommend using 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.

Product and Subsystem Security


Topics:

- [Security Controls Map](#)
- [Authentication](#)
- [Login security settings](#)
- [Authentication types and setup considerations](#)
- [User and credential management](#)
- [Network security](#)
- [Data security](#)
- [Cryptography](#)
- [Auditing and logging](#)
- [Serviceability](#)
- [OMIMSSC Operating System update](#)
- [Product code integrity](#)

Security Controls Map

OMIMSSC performs deployment, inventory, and update of PowerEdge and MX 7000 chassis using iDRAC. iDRAC can communicate with appliance over HTTPS and NFS for different system related updates.

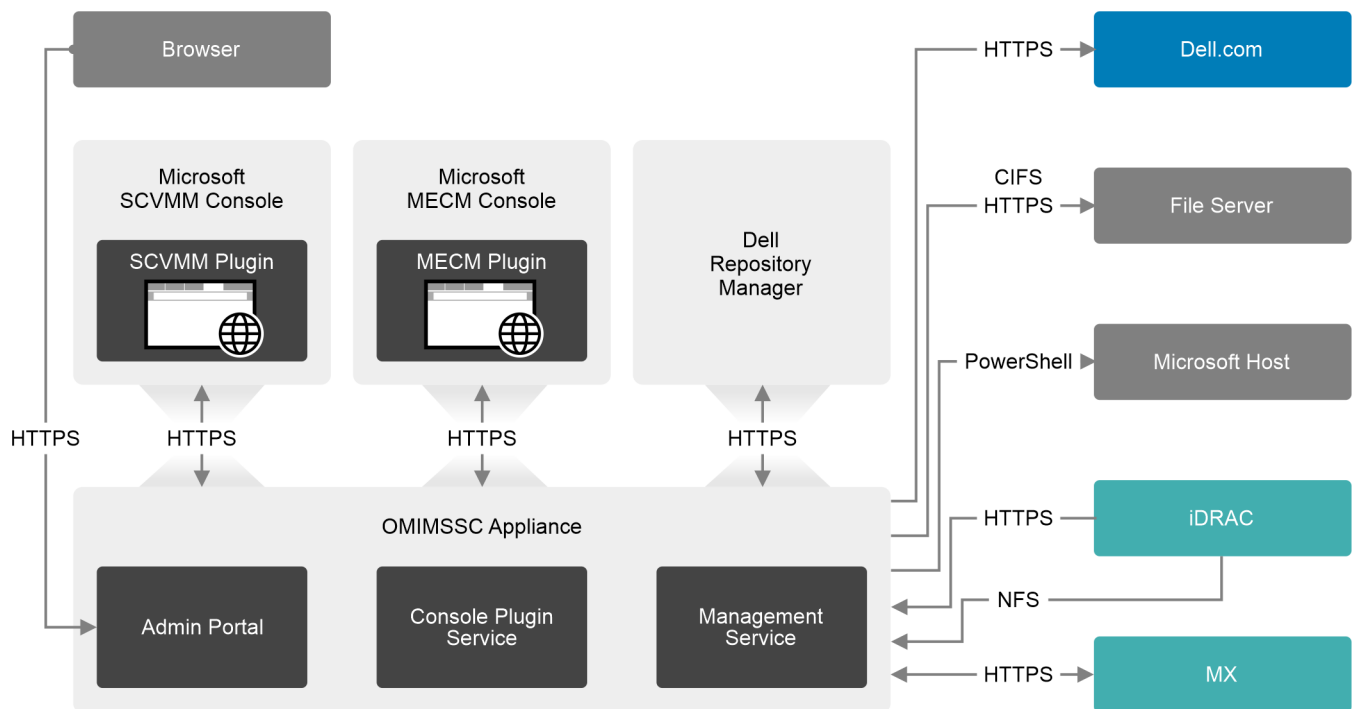
The User Interface of OMIMSSC is the appliance administration web page. The OMIMSSC plugin UI operates from Microsoft System Center consoles and provides host hardware management capabilities.

 **NOTE:** A single OMIMSSC appliance can be used for both MECM and SCVMM consoles.

Credentials to access managed nodes and Microsoft system center consoles are stored in an encrypted format in the database. OMIMSSC appliance interacts over Powershell with MECM and SCVMM for information sync up and interacts with managed nodes for cluster aware update.

The following figure displays the OMIMSSC security controls map:

Security Controls Map



Authentication

Access control

Access control settings provide protection of resources against unauthorized access. OMIMSSC plug-in pages accessed by Microsoft System Center console users with appropriate roles and privileges configured in Microsoft Active Directory. OMIMSSC administration console access is given to OMIMSSC appliance admin account.

For more information on roles and privileges see, User Credential Management and Authorization.

OMIMSSC Appliance administration

Default user accounts

OMIMSSC includes the following default user accounts:

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

Local user account (Admin account)

OMIMSSC 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 administration console 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

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

The user with readonly permissions can log in to OMIMSSC using the VM remote console only.

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

Root account

OMIMSSC 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](#).

Infrastructure administration using Microsoft System Center Console

Microsoft System Center 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 OMIMSSC console extension when the console users have appropriate roles and privileges on Microsoft Active Directory.

OMIMSSC provide integration with following Microsoft System Center Consoles :

Microsoft Endpoint Configuration Manager

Configuration Manager uses role-based administration to help secure objects like collections, deployments, and sites. This administration model centrally defines and manages hierarchy-wide security access settings for all sites and site settings.

The role-based administration model centrally defines and manages hierarchy-wide security access.

For more information about roles and privileges in Microsoft Endpoint Configuration Manager, see <https://docs.microsoft.com/en-us/mem/configmgr/core/understand/fundamentals-of-role-based-administration>

Microsoft System Center Virtual Machine Manager

Microsoft System Center - Virtual Machine Manager (VMM) allows you to manage roles and permissions as follows. OMIMSSC console extension uses the Virtual Machine Manager SCVMM Console add-ins Framework to interact with OMIMSSC appliance.

Role-based security:

Roles specify what users can do in the VMM environment. 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.

Run As accounts:

Run As accounts act as containers for stored credentials that you use to run VMM tasks and processes.

For more information about roles and privileges in Microsoft System Center Virtual Machine Manager see, [Microsoft documentation](#).

Login security settings

OMIMSSC Appliance administration

OMIMSSC console use local user account (admin account) to access OMIMSSC administration portal and virtual appliance. It validates the user authentication on appliance. Admin account have logout option post administration operations are completed. On administration 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 supported multiple logins for admin account and each account login has separate session.

Failed login behavior

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

Local user account logout

After 3 consecutive failed attempts to login to the local user account, OMIMSSC 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 administration using Microsoft System Center Console

Failed login behavior

OMIMSSC leverages Microsoft Active Directory to verify the authentication and authorization of the user. OMIMSSC console plugin extension login page shows appropriate error message for unsuccessful authentication occurrences. For invalid login attempts the user prompted with `Failed to login. Ensure to use correct credentials or check if account is locked in Active Directory` message.

Microsoft System Center Console user account logout

OMIMSSC leverages Microsoft Active Directory to verify the validity of the user. Account lockout policies configured in Active Directory can temporarily lock out the user for a set period as defined by lockout policies. OMIMSSC console plugin extension login page shows appropriate error message when there are unsuccessful authentication occurrences due to account lockout.

For more information about roles and privileges in Microsoft Endpoint Configuration Manager, follow the links below Windows Server <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/ad-fs-password-protection>

Automatic session timeout

Idle browser timeout

The session timeout is applicable for session created with OMIMSSC console extension user. By default, after 15 minutes of inactivity, the OMIMSSC console plugin extension's session times out and you are automatically logged out. For more information about roles and privileges see, [User and credential management](#).

Authentication types and setup considerations

OMIMSSC Appliance administration

Authentication types

OMIMSSC supports basic username and password-based authentication. OMIMSSC appliance credentials are stored in appliance in secured manner. Admin user can login to admin portal and appliance VM console using valid credentials.

Setup considerations

OMIMSSC admin operations for setup

Admin account perform following operations to integrate with Microsoft System Center Consoles.

Download OMIMSSC console extension

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 Download Installer to download the required console extension.

For more information about download OMIMSSC console extension, see the *OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager 7.3 User's Guide* available at <https://www.dell.com/support>.

Enroll Microsoft System Center consoles in OMIMSSC

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 with Microsoft System Center Consoles.

For more information about Enrollment with Microsoft System Center Console, see the *OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager 7.3 User's Guide* available at <https://www.dell.com/support>.

OMIMSSC appliance uses Windows PowerShell Remoting to run PowerShell commands on Microsoft System Center Consoles. Enrollment process used PowerShell cmdlet internally to authenticate and authorize Microsoft System Center user. It creates application profile on respective System Center console to provide the launch point for OMIMSSC console extension. For more information on PowerShell remoting, see Windows PowerShell Remoting.

Infrastructure administration using Microsoft System Center Console

Authentication types

OMIMSSC console extension support 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 Microsoft System Center consoles from appliance are created through credential profile and stored on OMIMSSC appliance.

Setup considerations

OMIMSSC console extension operations for setup

OMIMSSC console extension provides interface in Microsoft System Center consoles to access OMIMSSC appliance in console plugin OMIMSSC appliance provide login page for the Microsoft System Center Console Users.

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

A user with valid privileges can perform OMIMSSC console extension installation. For more information about Enrollment of Microsoft System Center Console, see Microsoft System Center user account privileges

Install OMIMSSC console extension

Microsoft System Center Console user with software installation privilege can install the OMIMSSC console extensions. OMIMSSC console extensions in case of MECM and Add-in plugin in case of SCVMM create appropriate folders on the host

For more information about console extension installation, see the *OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager 7.3 User's Guide* available at <https://www.dell.com/support>.

Launch OMIMSSC console extension for Microsoft System Center Consoles

Microsoft System Center Console user must have the Microsoft System Center access and privilege to launch the OMIMSSC Console Extension. OMIMSSC console extensions in case of MECM and Add-in plugin in case of SCVMM create appropriate folders on the host.

For more information about launching console extension, see the *OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager 7.3 User's Guide* available at <https://www.dell.com/support>.

Access OMIMSSC appliance from enrolled Microsoft console

Security roles and permissions

The OpenManage Integration for Microsoft System Center Version 7.3 for System Center Configuration Manager and System Center Virtual Machine Manager 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 stored in CIFS. CIFS share provided by authorized user. CIFS share accessed using credential by authorized users. Backup operation expect user provided password for additional protection. The backup password provided by user do not stored in the appliance hence user have to remember it and provide the same 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 OpenManage Integration for Microsoft System Center Version 7.3 for System Center Configuration Manager and System Center Virtual Machine Manager within Microsoft System Center Console Plugins.

Data integrity

The communication between the OMIMSSC appliance and Microsoft Endpoint Configuration Manager (MECM) and System Center Virtual Machine Manager (SCVMM) 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.

The communication between the Microsoft System Center Consoles and OMIMSSC appliance is over HTTPS. The OMIMSSC appliance generates a certificate that is used for trusted communication between MECM/SCVMM and the appliance.

Access control authentication, authorization, and roles

To perform operations on managed nodes by Microsoft System Center Consoles, OMIMSSC uses the current user session and authorization available in Microsoft System Center console.

OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager uses the Microsoft Active Directory (MS AD) built-in roles and privileges model to authorize user actions for managed server (hosts and clusters).

Windows PowerShell Remoting

Using the WS-Management protocol, Windows PowerShell Remoting lets you run any Windows PowerShell command on one or more remote computers. 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 *About Remote Requirements*.

To enable PowerShell Remoting, see PowerShell Permissions

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	User Name	Password	Description
Admin User	admin	Set on first boot after deployment. For more information about changing admin password, see Change OMIMSSC appliance password.	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 administration console, log in as an administrator (the default user name 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 administration using Microsoft System Center Console

Microsoft System Center Console users can access the OMIMSSC plugin User Interface elements from OMIMSSC Client when the users have appropriate roles and privileges on Microsoft Active Directory.

For more information about roles and privileges, see Microsoft System Center Console user privileges .


OMIMSSC uses predefined users in Microsoft Active Directory. OMIMSSC maintains the credential profiles to access Microsoft System Center consoles. Each profile mapped to single user in Microsoft Active Directory. For more information about credential profile management see, Credential profiles to access Microsoft System Center Consoles.

Credential profiles to access Microsoft System Center Consoles

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

You can create four types of credential profiles:

- Device Credential Profile-used to log in to iDRAC or CMC. Also, you can use this profile to discover a server, 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 accessing share folders in Windows operating system.
- Proxy Server Credentials-used for providing proxy credentials for accessing any FTP sites for updates.

 **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:

- Download console extension for MECM and SCVMM
- Import valid license
- Upgrade OMIMSSC appliance using RPM and backup and restore
- Restore OMIMSSC Appliance
- Backup OMIMSSC Appliance
- Generate a Certificate Signing Request (CSR)
- Upload HTTPS certificate
- Enrolled MECM and SCVMM consoles
- Generate and download the troubleshooting bundle
- For invalid login attempts the user prompted with `User Name or Password is incorrect` message.

Infrastructure administration using Microsoft System Center 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 OMIMSSC console extension.

Table 3. User accounts with required privileges

Users	Privileges/Roles
For enrollment	<ul style="list-style-type: none">Account used to enroll the MECM console with OMIMSSC should be a full admin or an administrator in MECM.Account used to enroll the SCVMM console with OMIMSSC should be a member of administrator role in SCVMM.Domain user.Member of Local Administrator group in system center machine.
For logging in to console extensions	<ul style="list-style-type: none">Account used to enroll the MECM console with OMIMSSC should be a full admin or an administrator in MECM.Account used to enroll the SCVMM console with OMIMSSC should be a delegated admin or an administrator in SCVMM.Domain user.Member of Local Administrator group in system center machine.

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.

Management Station Ports

Management station ports can be used by OMIMSSC when connecting to a remote system.

The following table lists the ports that are pre-configured with OMIMSSC management station's firewall.

Table 4. Ports OMIMSSC uses for listening

Port Number	Protocols	Port Type	Source	Direction	Destination	Usage	Description
80	HTTP	TCP	OMIMSSC Appliance (Browser Client System)	In/Out	OMIMSSC Appliance	Redirection from HTTP to HTTPS	Used for internal redirection communication.

Table 4. Ports OMIMSSC uses for listening (continued)

Port Number	Protocols	Port Type	Source	Direction	Destination	Usage	Description
111	HTTPS	TCP	iDRAC	In	OMIMSSC Appliance	NFS	Used to determine the address of the NFS.
443	HTTPS	TCP	OMIMSSC Admin Console and OMIMSSC Plugin Integrated Dashboard	In	OMIMSSC Appliance	HTTPS server	OMIMSSC Admin Console launched on remote browser & OMIMSSC Plugin Integrated Dashboard of MECM & SCVMM uses this port to connect with OMIMSSC Appliance.
2049	NFS	TCP/UDP	iDRAC	In	OMIMSSC Appliance	Public Share	NFS public share that is exposed by OMIMSSC appliance to the managed nodes and used in firmware update and operating system deployment flows.
4003	NFS	TCP/UDP	iDRAC	In	OMIMSSC Appliance	Public Share	These ports used for mountd service.
4433	HTTPS	TCP	iDRAC	In	OMIMSSC Appliance	Auto Discovery	Provisioning server that is used for auto discovering managed nodes.

Table 5. Ports OMIMSSC uses as client

Port Number	Protocols	Port Type	Source	Direction	Destination	Usage	Description
53	DNS	TCP/UDP	OMIMSSC Appliance	Out	DNS server	DNS Client	Connectivity to DNS server for resolving the host names
67, 68	DHCP	UDP	OMIMSSC Appliance	Out	DNS and DHCP	Dynamic network configuration	To get network details like IP, Gateway, Netmask, DNS and DHCP.
80	HTTP	TCP	OMIMSSC Appliance	Out	Internet	Dell Online Data Access	To connect to the service pack update repository of OMIMSSC.
139	CIFS	TCP	OMIMSSC Appliance	Out	CIFS supported Host	CIFS communication	To access the remote file system.
443	HTTPS	TCP	OMIMSSC Appliance	Out	Internet	HTTPS server	To connect to the online repository to download firmware.
445	CIFS	TCP	OMIMSSC Appliance	Out	CIFS supported Host	CIFS communication	To access the remote file system.

Table 5. Ports OMIMSSC uses as client (continued)

Port Number	Protocols	Port Type	Source	Direction	Destination	Usage	Description
2049	NFS	TCP/UDP	OMIMSSC Appliance	Out	OMIMSSC Appliance	Public Share	NFS public share that is exposed by OMIMSSC appliance to the managed nodes and used in firmware update and operating system deployment flows.
5985, 5986	HTTP/HTTPS	TCP/UDP	OMIMSSC Appliance	Out	Managed Node Host OS	PowerShell Connectivity between Appliance and Microsoft System Center consoles	Appliance connect to Host OS of MECM and SCVMM.

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 use AES-256 based encryption for data security.

The data in transit is protected using HTTPS protocol

Data at rest encryption

This section describe 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 have encryption key management in place as described below.

Generate Encryption Key

OMIMSSC support 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 in by performing change password for admin account. Similarly new encryption key will be used when appliance restored from one version to higher version.

For more information, see [Change OMIMSSC appliance admin password](#).

Sensitive Data Migration

About this task

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 provided password is used to protect the exported backup files.

Following are the steps to migrate data:

Steps

1. Backup the OMIMSSC appliance data using Admin portal. Backup data will be stored on CIFS share. CIFS share can be accessed by authorised 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 (internal) 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 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 *the OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager 7.3 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 *OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager Version 7.3 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 Tech support guides to check specific parameters.

Download troubleshooting bundle

Prerequisites

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

Steps

1. On the **Admin portal**, click **Logs** under **Settings** menu.
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.
3. 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 support and OMIMSSC users get notifications on the OMIMSSC upon the same.

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 RPM update package. When available, it is highly recommended that you install these security patches and fixes on the OMIMSSC server through RPM update.

Product code integrity

The OMIMSSC software installer is signed by Dell. Download software install from 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_v<version>.<build_number>_for_VMM_and_ConfigMgr_A00.zip file. The hash algorithm used is the default SHA256. 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>

Miscellaneous Configuration and Management

Topics:

- OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager (OMIMSSC) licensing
- Manage backup and restore in OMIMSSC
- PowerShell Permission
- Configuring user access to WMI for MECM

OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager (OMIMSSC) licensing

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 the Dell EMC servers.
- Standard 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 OMIMSSC from a disaster scenario, it is recommended that you perform backups of OMIMSSC. If required, you can restore OMIMSSC from these backups. For more information about backup and restore, see the OMIMSSC 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.


If the status is different, then perform the following steps in PowerShell:

- In PowerShell run the command: PSRemoting.
If the PSRemoting command is disabled, run enable the PSRemoting command using the following commands.
 - Run the command: Enable-PSRemoting.
 - In the confirmation message, type Y.
- In PowerShell, run the command: Get-ExecutionPolicy.
If the policy is not set to RemoteSigned, then set it to RemoteSigned using the following commands.
 - Run the command: Set-ExecutionPolicy RemoteSigned.
 - In the confirmation message, type Y.

Configuring user access to WMI for MECM

To configure user access to WMI remotely:

About this task

 **NOTE:** Make sure that firewall of the system does not block the WMI connection.

Steps

1. To access the Distributed Component Object Model (DCOM) remotely, provide permissions to the enrolled MECM user. To grant user permissions for DCOM:
 - Launch dcomcnfg.exe.
 - From the left pane, in the Component Services console, expand Computers, right-click My Computer, and select properties.
 - On COM Security:
 - From Access Permissions, click Edit Limits and select Remote Access.
 - From Launch and Activation Permission, click Edit Limits and select Local Launch, Remote Launch, and Remote Activation.
2. To access the DCOM Config Windows Management and Instrumentation (WMI) components, provide user permissions to the enrolled user. To grant user permissions for DCOM Config WMI:
 - Launch dcomcnfg.exe
 - Expand My Computer > DCOM Config.
 - Right- click Windows Management and Instrumentation and select Properties.
 - On Security, from Launch and Activation Permission, click Edit and select the Remote Launch and Remote Activation Permissions
3. Set the namespace security and grant permissions. To set namespace security and grant permissions:
 - Launch wimgmt.msc.
 - In WMI Control pane, right-click WMI Control, select Properties, and then select Security.
 - Navigate to ROOT\SMS Namespace.
 - Select the Execute Methods, Provider Write, Enable Account, and the Remote Enable permissions.
 - Navigate to Root\cimv2\OMIMSSC.
 - Select the Execute Methods, Provide Write, Enable Account, and the Remote Enable permissions .

Alternatively, the Configuration Manager user becomes a member of the SMS_Admin group, and you can grant Remote Enable to the existing permissions of the group.