Dell EMC OpenManage Version 9.0.1 Installation Guide — Microsoft Windows

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.

Copyright

2017 - 06

Rev. A00

Contents

1

Introduction

This topic provides information on:

- Installing Server Administrator on managed systems.
- Installing and using the Remote Enablement feature.
- Managing remote systems using Server Administrator Web Server.
- Configuring the system before and during a deployment or upgrade.

NOTE: If you are installing management station and managed system software on the same system, install identical software versions to avoid system conflicts.

What Is New In This Release

The release highlights of Server Administrator are:

- Full Power Cycle.
- System Lockdown mode.
- NVDIMM Monitoring.
- Support for the following browsers:
  - Internet Explorer - 9, 10, 11
  - Microsoft Edge 25
  - Google Chrome - 58
  - Safari - 9.1
  - Mozilla Firefox - 52, 53
- Support for Java Runtime Environment 8 Update 112.
- SD card support for 32 GB and 64 GB.

For related document, see Other Documents You Might Need.

NOTE: For the list of supported operating systems and servers, see the *Dell EMC OpenManage Software Support Matrix* in the required version of OpenManage Software at dell.com/openmanagemanuals.

Software Availability

The Server Administrator software can be installed from:

- Systems Management Tools and Documentation software
- Support site — For more information, see **dell.com/support/home**.

Systems Management Software

Systems management software is a suite of applications that enables you to manage the systems with proactive monitoring, notification, and remote access.

Systems management software comprises of two ISO images:

- *Systems Management Tools and Documentation*
- *Server Update Utility*

NOTE: For more information on these ISO images, see *Systems Management Tools And Documentation Installation Guide*.

Server Administrator Components On A Managed System

The setup program provides the following options:

- Custom Setup
- Typical Setup

The custom setup option allows you to select the software components you want to install. The table lists the various managed system software components that you can install during a custom installation.

Table 1. Managed System Software Components

Component	What is installed	Deployment Scenario	Systems to install on
Server Administrator Web Server	Web-based Systems Management functionality that enables you to manage systems locally or remotely.	Install only if you want to remotely monitor the managed system. You do not require physical access to the managed system.	Any system. For example, laptop or desktops.
Server Instrumentation	Server Administrator Instrumentation Service	Install to use the system as the managed system. Installing Server Instrumentation and the Server Administrator Web Server installs Server Administrator. Use Server Administrator to monitor, configure, and manage the system. **NOTE: If you choose to install only Server Instrumentation, you must also install one of the Management Interfaces or the Server Administrator Web Server.**	Supported systems. For a list of supported systems, see the *Dell EMC OpenManage Systems Software Support Matrix* at **dell.com/support/manuals.**
Storage Management	Server Administrator Storage Management	Install to implement hardware RAID solutions and configure the storage components attached to the system. For more information on Storage Management, see the *Dell EMC OpenManage Server Administrator Storage Management User's Guide* in the docs directory.	Only those systems on which you have installed Server Instrumentation or the Management Interfaces.
Command Line Interface (Management Interface)	Command Line Interface of Server Instrumentation	Install to provide local and remote system management solutions to manage Server and Storage instrumentation data using command-line interfaces.	Supported systems. For a list of supported systems, see the *Dell EMC OpenManage Systems Software Support Matrix*.

Component	What is installed	Deployment Scenario	Systems to install on
WMI (Management Interface)	Windows Management Instrumentation Interface of Server Instrumentation	Install to provide local and remote system management solutions to manage Server data using WMI protocol.	Supported systems. For a list of supported systems, see the *Dell EMC OpenManage Systems Software Support Matrix*.
SNMP (Management Interface)	Simple Network Management Protocol Interface of Server Instrumentation	Install to provide local and remote system management solutions to manage Server and Storage instrumentation data using SNMP protocol.	Supported systems. For a list of supported systems, see the *Dell EMC OpenManage Systems Software Support Matrix*.
Remote Enablement (Management Interface)	Instrumentation Service and CIM Provider	Install to perform remote systems management tasks. Install Remote Enablement on one system and Server Administrator Web Server on another system. You can use the system with the Server Administrator to remotely monitor and manage the systems which have Remote Enablement installed.	Supported systems. For a list of supported systems, see the *Dell EMC OpenManage Systems Software Support Matrix*.
Operating System Logging (Management Interface)	Operating System Logging	Install to allow local system management-specific events logging on the operating system for Server and Storage instrumentation. On systems running Microsoft Windows, use the Event Viewer to locally view the collected events.	Supported systems. For a list of supported systems, see the *Dell EMC OpenManage Systems Software Support Matrix*.
iDRAC Command Line Tools	Hardware application programming interface and iDRAC (depending on the type of the system)	Install to receive email alerts for warnings or errors related to voltage, temperature, and fan speed. Remote Access Controller also logs event data and the most recent crash screen (available only on systems running Windows operating system) to help you diagnose the probable cause of a system crash.	Only those systems on which you have installed Server Instrumentation or Management Interface.
Intel SNMP Agent (NIC Interfaces)	Intel Simple Network Management Protocol (SNMP) Agent	Install to enable Server Administrator to obtain information about Intel Network Interface Cards (NICs).	Only on systems on which Server Instrumentation is installed and which are running on Windows operating system.
Broadcom SNMP Agent (NIC Interfaces)	Broadcom SNMP Agent	Install to enable Server Administrator to obtain information about Broadcom NICs.	Only on systems on which Server Instrumentation is installed and which are running on Windows operating system.
QLogic SNMP Agent (NIC Interfaces)	QLogic SNMP Agent	Install to enable Server Administrator to obtain information about QLogic NICs.	Only on systems on which Server Instrumentation is installed and which are running on Windows operating system.

Security Features

Systems management software components provide these security features:

- Authentication for users from operating system with different privilege levels, or by using the optional Microsoft Active Directory.
- User ID and password configuration through the web-based interface or the command line interface (CLI), in most cases.
- SSL encryption (**Auto Negotiate** and **128-bit or higher**).

NOTE: Telnet does not support SSL encryption.

- Session time-out configuration (in minutes) through the web-based interface.
- Port configuration to allow systems management software to connect to a remote device through firewalls.

NOTE: For information about ports that the various systems management components use, see the User Guide for that component.

For information about the Security Management, see the *Dell EMC OpenManage Server Administrator User's Guide* at **dell.com/openmanagemanuals**.

Other Documents You Might Need

In addition to this guide, for more information, access the following guides.

- The *Lifecycle Controller 2 Version 1.00.00 User's Guide* provides information on using the Lifecycle Controller.
- The *Dell EMC OpenManage Management Console User's Guide* provides information about installing, configuring, and using Management Console.
- The *Systems Build and Update Utility User's Guide* provides information on using the Systems Build and Update Utility.
- The *Dell EMC OpenManage Systems Software Support Matrix* provides information about the various systems, the operating systems supported by these systems, and the systems management components that can be installed on these systems.
- The *Dell EMC OpenManage Server Administrator User's Guide* describes the installation and use of Server Administrator.
- The *Dell EMC OpenManage Server Administrator SNMP Reference Guide* documents the SNMP management information base (MIB).
- The *Dell EMC OpenManage Server Administrator CIM Reference Guide* documents the Common Information Model (CIM) provider, which is an extension of the standard management object format (MOF) file. This guide explains the supported classes of management objects.
- The*Dell EMC OpenManage Server Administrator Messages Reference Guide* lists the messages that are displayed on the Server Administrator home page Alert log, or on the operating system's event viewer. This guide explains the text, severity, and cause of each alert message that the Server Administrator displays.
- The *Dell EMC OpenManage Server Administrator Command Line Interface Guide* documents the complete command line interface for Server Administrator, including an explanation of CLI commands to view system status, access logs, create reports, configure various component parameters, and set critical thresholds.
- The *Remote Access Controller User's Guide* provides complete information about installing and configuring a DRAC controller and using DRAC to remotely access an inoperable system.
- The *Integrated Remote Access Controller User's Guide* provides complete information about configuring and using an integrated Remote Access Controller to remotely manage and monitor the system and its shared resources through a network.
- The *Update Packages User's Guide* provides information about obtaining and using the Update Packages for Windows and Linux as part of the system update strategy.
- The *Server Update Utility User's Guide* provides information on using the Server Update Utility.
- The *Dell EMC OpenManage Systems Management Tools and Documentation* software contains readme files for applications found on the media.

NOTE: If the product does not perform as expected or you do not understand a procedure described in this guide, see Getting Help in the system's Hardware Owner's Manual.

2

Preinstallation Setup

Ensure that you perform the following before installing Server Administrator:

- Read the installation instructions for the operating system.
- Read the Installation Requirements to ensure that the system meets or exceeds the minimum requirements.
- Read the applicable readme files and the *Dell EMC OpenManage Systems Software Support Matrix*.
- Close all applications running on the system before installing the Server Administrator applications.

Prerequisite Checker

The **setup.exe** (available at **\SYSMGMT\srvadmin\windows**) starts the prerequisite checker program. The prerequisite checker program examines the prerequisites for software components without launching the actual installation. This program displays a status window that provides information about the system's hardware and software that may affect the installation and operation of software features.

NOTE: To use supporting agents for the Simple Network Management Protocol (SNMP), install the operating system support for the SNMP standard before or after you install Server Administrator. For more information about installing SNMP, see the installation instructions for the operating system you are running on the system.

Run the prerequisite checker silently by running `runprereqchecks.exe /s` from the **SYSMGMT\srvadmin\windows \PreReqChecker**directory on the *Systems Management Tools and Documentation* software. After running the prerequisite checker, an HTML file (**omprereq.htm**) is created in the **%Temp%** directory. This file contains the results of the prerequisite check. The **Temp** directory is at **X:\Documents and Settings\username\Local Settings\Temp**. To find **%TEMP%**, go to a command-line prompt and type `echo %TEMP%`.

The results are written under the **HKEY_LOCAL_MACHINE\Software\Dell Computer Corporation\OpenManage \PreReqChecks \MN** key for a managed system:

While running the prerequisite checker silently, the return code from **runprereqchecks.exe** is the number associated with the highest severity condition for all the software products. The return code numbers are the same as those used in the registry. The following table details the return codes.

Table 2. Return Codes While Running the Prerequisite Checker Silently

Return Code	Description
0	No condition, or conditions, is associated with the software.
1	An informational condition, or conditions, is associated with the software. It does not prevent a software product from being installed.
2	A warning condition, or conditions, is associated with the software. It is recommended that you resolve the conditions causing the warning before proceeding with the installation of the software. To continue, select and install the software using the custom installation.
3	An error condition, or conditions, is associated with the software. Resolve the conditions causing the error before proceeding with the installation of the software. If you do not resolve the issues, the software is not installed.
—1	A Microsoft Windows Script Host (WSH) error. The prerequisite checker does not run.
—2	The operating system is not supported. The prerequisite checker does not run.
—3	The user does not have **Administrator** privileges. The prerequisite checker does not run.
—4	Not an implemented return code.

Return Code	Description
—5	The prerequisite checker does not run. The user failed to change the working directory to **%TEMP%**.
—6	The destination directory does not exist. The prerequisite checker does not run.
—7	An internal error has occurred. The prerequisite checker does not run.
—8	The software is already running. The prerequisite checker does not run.
—9	The WSH is corrupted, is a wrong version, or is not installed. The prerequisite checker does not run.
—10	An error has occurred with the scripting environment. The prerequisite checker does not run.

NOTE: A negative return code (-1 through -10) indicates a failure in running the prerequisite checker tool. Probable causes for negative return codes include software policy restrictions, script restrictions, lack of folder permissions, and size constraints.

NOTE: If you encounter a return code of 2 or 3, it is recommended that you inspect the omprereq.htm file in the windows temporary folder %TEMP%. To find %TEMP%, run `echo %TEMP%`.

Common causes for a return value of 2 from the prerequisite checker:

- One of the storage controllers or drivers has outdated firmware or driver. See **firmwaredriverversions_<lang>.html** (where < *lang* > stands for language) or **firmwaredriverversions.txt** found in the **%TEMP%** folder. To find **%TEMP%**, run `echo %TEMP%`.
- RAC component software version 4 is not selected for a default install unless the device is detected on the system. The prerequisite checker generates a warning message in this case.
- Intel, Broadcom, and QLogic agents are selected for a default install only if the corresponding devices are detected on the system. If the corresponding devices are not found, prerequisite checker generates a warning message.
- Domain Name System (DNS) or Windows Internet Name Service (WINS) server running on the system can cause a warning condition for RAC software. See the relevant section in Server Administrator readme for more information.
- Do not install managed system and management station RAC components on the same system. Install only the managed system RAC components, as they offer the required functionality.

Common causes for a return code of 3 (failure) from the prerequisite checker:

- You are not logged in as a built-in **Administrator**, Domain Administrator, or user who is a part of **Domain Admins** and **Domain Users** group.
- The MSI package is corrupt or one of the required XML files is corrupt.
- Error during copying from a DVD or network access problems while copying from a network share.
- Prerequisite checker detects that another MSI package installation is running or that a reboot is pending: HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\Windows\CurrentVersion\Installer\InProgress indicates that another MSI package installation is in progress. HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Session Manager\ \PendingFileRenameOperations indicates that a reboot is pending.
- Running the 64-bit version of Windows Server 2008 Core, since certain components are disabled from being installed.

Ensure that any error or warning is corrected before you proceed to install systems management software components.

Related Link

Customization Parameters

Installation Requirements

This section describes the general requirements of the Server Administrator and provides information on supported operating systems and web browsers.

NOTE: Prerequisites specific to an operating system are listed as part of the installation procedures.

Supported Operating Systems And Web Browsers

For information on supported operating systems and web browsers, see the *Dell EMC OpenManage Systems Software Support Matrix* .

NOTE: Ensure that the web browser is configured to bypass the proxy server for local addresses.

Multilingual User Interface Support

The installer provides Multilingual User Interface (MUI) support available on the following operating systems:

- Microsoft Windows Server 2016

The MUI Pack are a set of language-specific resource files that you can add to the English version of a supported Windows operating system. The installer supports only six languages: English, German, Spanish, French, Simplified Chinese, and Japanese.

NOTE: When the MUI Pack is set to non-Unicode languages like Simplified Chinese, set the system locale to Simplified Chinese. This enables display of the prerequisite checker messages. This is because any non-Unicode application runs only when the system locale (also called Language for non-Unicode Programs on XP) is set to match the application's language.

Viewing Localized Versions Of The Web-Based Interface

To view the localized versions of the web interface on Windows, in the **Control Panel** select **Regional and Language Options**.

System Requirements

Install Server Administrator on each system to be managed. You can manage systems running Server Administrator locally or remotely through a supported web browser.

Managed System Requirements

- One of the supported operating systems and web browser.
- Minimum 2GB RAM.
- Minimum 512MB free hard drive space.
- Administrator rights.
- TCP/IP connection on the managed system and the remote system to facilitate remote system management.
- One of the Supported Systems Management Protocol Standards.
- Monitor with a minimum screen resolution of 800 x 600. The recommended screen resolution is at least 1024 x 768.
- The Server Administrator Remote Access Controller service requires remote access controller (RAC) installed on the managed system. See the relevant *Remote Access Controller User's Guide* for complete software and hardware requirements.

  NOTE: The RAC software is installed as part of the Typical Setup installation option, provided the managed system meets all of the RAC installation prerequisites.
- The Server Administrator Storage Management Service requires Server Administrator installed on the managed system. See the *Dell EMC OpenManage Server Administrator Storage Management User's Guide* for complete software and hardware requirements.

Related Link:

Supported Systems Management Protocol Standards

Install a supported systems management protocol on the managed system before installing the management station or managed system software. On supported Windows operating system, systems management software supports:

- Common Information Model (CIM)/Windows Management Instrumentation (WMI)
- Simple Network Management Protocol (SNMP)

Install the SNMP package provided with the operating system. If SNMP is installed post Server Administrator installation, restart Server Administrator services.

NOTE: For information about installing a supported systems management protocol standard on the managed system, see the operating system documentation.

The following table shows the availability of the systems management standards for each supported operating system.

Table 3. Availability of Systems Management Protocol by Operating Systems

Operating System	SNMP	CIM/WMI
Supported Microsoft Windows operating systems.	Available from the operating system installation media.	Always installed.

Digital Certificates

All Server Administrator packages for Microsoft are digitally signed with a certificate that helps guarantee the integrity of the installation packages. If these packages are repackaged, edited, or manipulated in other ways, the digital signature is invalidated. This manipulation results in an unsupported installation package and the prerequisite checker does not allow you to install the software.

Enabling Windows Installer Logging Service

Windows includes a registry-activated logging service to help diagnose Windows Installer issues.

To enable this logging service during a silent install, open the registry editor and create the following path and keys:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
Reg_SZ: Logging
Value: voicewarmup
```

The letters in the value field can be in any order. Each letter turns on a different logging mode. Each letter's actual function is as follows for MSI version 3.1:

v — Verbose output

o — Out-of-disk-space message

i —Status message

c — Initial UI parameter

e — All error message

w — Non-fatal warning

a — Startup of action

r — Action-specific record

m — Out-of-memory or fatal exit information

u — User request

p — Terminal property

+ — Append to existing file

! — Flush each line to the log

"*" — Wildcard, log all information except for the v option. To include the v option, specify "/l*v".

Once activated, the log files are generated in the **%TEMP%** directory. Some log files generated in this directory are:

- **Managed System Installation**
  - **SysMgmt_<timestamp>.log**

These log files are created by default if the prerequisite checker user interface (UI) is running.

Microsoft Active Directory

If you use Active Directory service software, you can configure it to control access to the network. The Active Directory database is modified to support remote management authentication and authorization. Server Administrator, Integrated Remote Access Controller (iDRAC), Chassis Management Controller (CMC), and Remote Access Controllers (RAC), can interface with Active Directory. Using Active Directory, add and control users and privileges from a central database.

Related Links:

Using Microsoft Active Directory

Configuring SNMP Agents

The systems management software supports the SNMP systems management standard on all supported operating systems. The SNMP support may or may not be installed depending on the operating system and how the operating system was installed. An installed supported systems management protocol standard, such as SNMP, is required before installing the systems management software.

Configure the SNMP agent to change the community name, enable set operations, and send traps to a management station. To configure the SNMP agent for proper interaction with management applications, perform the procedures described in the *Dell EMC OpenManage Server Administrator User's Guide*.

Related Links:

- Installation Requirements
- Supported Systems Management Protocol Standards

Secure Port Server And Security Setup

This section contains the following topics:

- Setting User and Server Preferences
- x 509 Certificate Management

Setting User And Server Preferences

You can set user and secure port server preferences for Server Administrator from the **Preferences** web page. Click **General Settings** and click either the **User** tab or **Web Server** tab.

X.509 Certificate Management

Web certificates are necessary to ensure that the identity and information exchanged with a remote system is not viewed or changed by others. To ensure system security, it is strongly recommended that you either generate a new X.509 certificate, reuse an existing X.509 certificate, or import a root certificate or certificate chain from a Certificate Authority (CA). Authorized CAs include Verisign, Entrust, and Thawte.

NOTE: Log in with administrator privileges to perform certificate management.

You can manage X.509 certificates for Server Administrator from the **Preferences** page. Click **General Settings**, select the **Web Server** tab, and click **X.509 Certificate**.

Best Practices For X.509 Certificate Management

For the security of the system while using server administrator, ensure the following:

Unique host name	All systems that have Server Administrator installed should have unique host names.
Change 'localhost' to unique	For systems with host name set to **localhost** change the host name to a unique host name.

Remote Enablement Requirements

The Remote Enablement feature is currently supported on:

- Microsoft Windows
- Microsoft Hyper-V
- Hyper-V Server

To install the Remote Enablement feature, configure the following on the system:

- Windows Remote Management (WinRM)
- CA/Self-Signed Certificate
- WinRM HTTPS Listener Port
- Authorization for WinRM and Windows Management Instrumentation (WMI) Servers

Installing WinRM

On Windows Server, Windows client operating system, and WinRM 2.0 is installed by default. On Windows Server, WinRM 1.1 is installed by default.

Certificate Authority Signed Self-Signed Certificate

You need a certificate signed by a CA or a self-signed certificate (generated using the SelfSSL tool) to install and configure the Remote Enablement feature on the system.

NOTE: It is recommended that you use a certificate signed by a CA.

Using A Certificate Signed By A CA

To use a certificate signed by a CA:

1. Request a valid CA signed certificate.
2. Create a HTTP listener with the CA signed certificate.

Requesting A Valid CA Signed Certificate

To request a valid CA signed certificate:

1. Click **Start** → **Run**.
2. Type **mmc** and click **OK**.
3. Click **File** → **Add/Remove Snap-in**.
4. Select **Certificates**, and then click **Add**.
5. In the **Certificates snap-in** dialog box, select **Computer account**, and then click **Next**.
6. Select **Local Computer**, and then click **Finish**.
7. Click **Close**, and then click **OK**.
8. On the **Console window**, expand **Certificates (Local Computer)** in the left navigation pane.
9. Right-click **Personal**, select **All tasks** → **Request New Certificate.**
10. Click **Next**.
11. Select the appropriate certificate type, **Mostly (Computer)**, and then click **Enroll**.
12. Click **Finish**.

Creating The HTTPS Listener With The Valid CA Signed Certificate

Run the installer and click the link on the prerequisite checker to create the HTTPS listener.

NOTE: The HTTP listener is enabled by default and listens at port 80.

Configuring User Authorization For WinRM And WMI Servers

To provide access rights to WinRM and WMI services, explicitly add users with the appropriate access levels.

NOTE: To configure user authorization — For WinRM and WMI Servers, you must login with administrator privileges. - For Windows Server operating systems, you must login as a built-in Administrator, Domain Administrator, or user who is a part of Domain Admins and Domain Users group.

NOTE: The administrator is configured by default.

WinRM

To configure user authorization for WinRM servers:

1. Click **Start** → **Run**.
2. Type `winrm configsddl` and click **OK**.

If you are using WinRM 2.0, type `winrm configsddl default`.

3. Click **Add** and add the required users or groups (local/domain) to the list.
4. Provide the appropriate permission(s) to the respective users and click **OK**.

WMI

To configure user authorization for WMI servers:

1. Click **Start** → **Run**.
2. Type `wmimgmt.msc`, and then click **OK**.

   The **Windows Management Infrastructure (WMI)** screen is displayed.
3. Right-click the **WMI Control (Local)** node in the left pane, and then click **Properties**.

   The **WMI Control (Local) Properties** screen is displayed.
4. Click **Security** and expand the **Root** node in the namespace tree.
5. Navigate to **Root** → **DCIM** → **sysman**.
6. Click **Security**.

   The **Security** screen is displayed.
7. Click **Add** to add the required users or groups (local/domain) to the list.
8. Provide the appropriate permission(s) to the respective users, and then click **OK**.
9. Click **OK**.
10. Close the **Windows Management Infrastructure (WMI)** screen.

Configuring The Windows Firewall For WinRM

To configure the Windows Firewall for WinRM:

1. Open **Control Panel**.
2. Click **Windows Firewall**.
3. Click **Exceptions** tab.
4. Select **Windows Remote Management** check box. If you do not see the check box, click **Add Program** to add Windows Remote Management.

Configuring The Envelope Size For WinRM

To configure the envelope size for WinRM:

NOTE: On WinRM version 2.0, enable the compatibility mode for WinRM version 2.0 to use port 443. WinRM version 2.0 uses port 5986 by default. To enable the compatibility mode, type the following command:

```
winrm s winrm/config/Service @{EnableCompatibilityHttpsListener="true"}
```

1. Open a command prompt.
2. Type `winrm g winrm/config`.
3. Check the value of the **MaxEnvelopeSizekb** attribute. If the value is less than **4608**, type the following command:

   ```
   winrm s winrm/config @{MaxEnvelopeSizekb="4608"}
   ```
4. Set the value of **MaxTimeoutms** to 3 minutes:

   ```
   winrm s winrm/config @{MaxTimeoutms ="180000"}
   ```

3

Installing Managed System Software On Microsoft Windows Operating Systems

On Microsoft Windows, an autorun utility is displayed when you insert the *Dell EMC OpenManage Systems Management Tools and Documentation* software. This utility allows you to choose the systems management software you want to install on the system.

If the autorun program does not start automatically, use the autorun program from the DVD root or the setup program in the SYSMGMT\srvadmin\windows directory on the *Dell EMC OpenManage Systems Management Tools and Documentation* software. See the *Dell EMC OpenManage Systems Software Support Matrix* for a list of operating systems currently supported.

NOTE: Use the *Dell EMC OpenManage Systems Management Tools and Documentation* software to perform an unattended and scripted silent installation of the managed system software. Install and uninstall the features from the command line.

Deployment Scenarios For Server Administrator

You can install Server Administrator in the following ways:

- Install the Server Administrator Web Server on any system (laptop, or desktop) and the Server Instrumentation on another supported system.

  In this method, the Server Administrator Web Server performs the function of a central web server and you can use it to monitor a number of managed systems. Using this method reduces the Server Administrator footprint on the managed systems.
- Continue to install the Server Administrator Web Server and the Server Instrumentation on the same system.

The following table lists the deployment scenarios for installing and using Server Administrator and helps you make the right choice while selecting the various installation options:

Table 4. Deployment Scenarios

You want to	Select
Remotely manage and monitor the entire network of managed systems from the system (laptop, desktop, or server).	**Server Administrator Web Server**. You must then install Server Instrumentation on the managed systems.
Manage and monitor the current system on the Web User Interface.	**Server Administrator Web Server** and **Server Instrumentation**.
Manage and monitor the current system on the Command Line Interface.	**Server Instrumentation** and **Command Line Interface**.
Manage and monitor the current system on the Windows Management Instrumentation Interface.	**Server Instrumentation** and **WMI**.
Manage and monitor the current system on the Simple Network Management Protocol Interface.	**Server Instrumentation** and **SNMP**.
Manage and monitor the current system from a remote system.	**Remote Enablement** For systems running on Microsoft Windows, **Remote Enablement** is under the **Server Instrumentation** option. You must then install the Server Administrator Web Server on the remote system.
View the status of local and remote storage attached to a managed system and obtain storage management information in an integrated graphical view.	**Storage Management**.

You want to	Select
Remotely access an inoperable system, receive alert notifications when a system is down, and remotely restart a system.	**iDRAC Command Line Tools**.

NOTE: Install the Simple Network Management Protocol (SNMP) agent on the managed system using the operating system medium before installing the managed system software.

Installer Location

The location of the installers is:

- DVD Drive\SYSMGMT\srvadmin\windows\SystemsManagementx64\SysMgmtx64.msi

Installing Server Administrator

This section explains how to install the Server Administrator and other managed system software using two installation options:

- Using the setup program at **\SYSMGMT\srvadmin\windows** on the *Dell EMC OpenManage Systems Management Tools and Documentation* software.
- Using the unattended installation method through the Windows Installer Engine **msiexec.exe**.

NOTE: SNMP service is stopped and started during Systems Management installation and uninstallation. As a result, other third-party services, dependent on SNMP stop. If the third-party services are stopped, manually restart the services.

NOTE: For Blade systems,install Server Administrator on each server module installed in the chassis.

NOTE: During installation of Server Administrator on supported Windows systems, if an Out of Memory error message is displayed, exit the installation and free up memory. Close other applications or perform any other task that frees up memory, before reattempting Server Administrator installation.

NOTE: If you use the MSI file to try to install Server Administrator on a system where the User Account Control settings is set to a greater level, the installation fails and displays a message: `Server Administrator installation program could not install the HAPI driver`. You must perform the installation process as an administrator. You can also install Server Administrator successfully by the following methods:

- Click the **setup.exe** file, or
- Right-click **Command Prompt** → **Run as administrator**, and then run the installer command in CLI mode. For more information on CLI mode, see Installing Managed System Software In CLI Mode

The setup program invokes the prerequisite checker, which uses the system's Peripheral Component Interconnect (PCI) bus to search for installed hardware such as controller cards.

The Systems Management installer features a **Typical Setup** option and a **Custom Setup** option for installing Server Administrator and other managed system software.

Related Links:

- Deployment Scenarios for Server Administrator
- Optional Command Line Settings

Typical Installation

When you access the Server Administrator installation from the prerequisite checker and select the **Typical Setup** option, the setup program installs the following managed system software features:

- Server Administrator Web Server
- Server Instrumentation
- Storage Management
- Command Line Interface
- WMI

- SNMP
- Operating System Logging
- DRAC Command Line Tools
- Intel SNMP Agent
- Broadcom SNMP Agent
- QLogic SNMP Agent

During a **Typical** installation, individual management station services that do not meet the specific hardware and software requirement for that service are not installed on the managed systems. For example, the Server Administrator Remote Access Controller service software module is not installed during a **Typical** installation unless the managed system has a remote access controller installed on it. You can, however, go to **Custom Setup** and select the **DRAC Command Line Tools** software module for installation.

NOTE: To install the drivers successfully, the installer runs in an elevated privilege mode.

NOTE: The Remote Enablement feature is available only through the Custom Setup option.

NOTE: Server Administrator installation also installs some of the required Visual C++ runtime components on the system.

NOTE: You can change the alert message format from Traditional Message Format to Enhanced Message Format using the Custom Setup option.

Custom Installation

The sections that follow describe how to install Server Administrator and other managed system software using the **Custom Setup** option.

NOTE: Management station and managed system services can be installed in the same or in different directories. You can select the directory for installation.

NOTE: To install the drivers successfully, the installer runs in an elevated privilege mode.

To perform a custom installation:

1. Log in as a built-in **Administrator**, Domain Administrator, or user who is a part of **Domain Admins** and **Domain Users** group, to the system on which you want to install the system management software.
2. Close all open applications and disable any virus-scanning software.
3. Mount the *Dell EMC OpenManage Systems Management Tools and Documentation* software into the system's DVD drive. The autorun menu is displayed.
4. Select **Server Administrator** from the autorun menu and click **Install**.

   The **Server Administrator** prerequisite status screen is displayed and runs the prerequisite checks for the managed system. Any relevant informational, warning, or error messages are displayed. Resolve all error and warning situations, if any.
5. Click the **Install, Modify, Repair, or Remove Server Administrator** option.

   The **Welcome to the Install Wizard for Server Administrator** screen is displayed.
6. Click **Next**.

   The **Software License Agreement** is displayed.
7. Click **I accept the terms in the license agreement** and then click **Next**.

   The **Setup Type** dialog box is displayed.
8. Select **Custom** and click **Next**.

   The **Custom Setup** dialog box is displayed.
9. Select the required software features you want to install on the system.

   If you are installing Server Administrator on an unsupported system, the installer displays only the **Server Administrator Web Server** option.

   A selected feature has a hard drive icon depicted next to it. A feature that is not selected has a red **X** depicted next to it. By default, if the prerequisite checker finds a software feature with no supporting hardware, the prerequisite checker automatically ignores the feature.

   To accept the default directory path to install managed system software, click **Next**. Else, click **Change** and browse to the directory where you want to install the managed system software, and click **OK**.

10. Click **Next** on the **Custom Setup** dialog box to accept the selected software features for installation.

    NOTE: You can cancel the installation process by clicking Cancel. The installation rolls back the changes that you made. If you click Cancel after a certain point in the installation process, the installation may not roll back properly, leaving the system with an incomplete installation.

    The **Alert Messaging Type Selection** dialog box is displayed.

11. Select one of the following options from the **Alert Messaging Type Selection** dialog box.

    - **Enhanced Message Format** (Recommended)
    - **Traditional Message Format**

    The **Ready to Install the Program** dialog box is displayed.

12. Click **Install** to install the selected software features.

    The **Installing Server Administrator** screen is displayed and provides the status and progress of the software features being installed. After the selected features are installed, the **Install Wizard Completed** dialog box is displayed with the following message. `iDRAC is an out-of-band management system that allows system administrators to monitor and manage PowerEdge Servers and other network equipment, remotely. iDRAC works regardless of Power status and operating system functionality. For more information, visit http://pilot.search.dell.com/iDRAC.`

13. Click **Finish** to exit the Server Administrator installation.

    If you are prompted to reboot the system, select from the following reboot options to make the installed managed system software services available for use:

    - **Yes, reboot my system now**.
    - **No, I will reboot my system later**.

NOTE: If you have selected Remote Enablement during installation, an error message `A provider, WinTunnel, has been registered in the Windows Management Instrumentation namespace ROOT\dcim\sysman to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.` is logged in Windows Event Log. You can safely ignore this message and continue with installation.

Related Links:

System Recovery on Failed Installation

Performing An Unattended Installation Of Managed System Software

The Systems Management installer features a **Typical Setup** option and a **Custom Setup** option for the unattended installation procedure.

Unattended installation enables you to simultaneously install Server Administrator on multiple systems. Perform an unattended installation by creating a package that contains the necessary managed system software files. The unattended installation option also provides several features that enable you to configure, verify, and view information about unattended installations.

The unattended installation package is distributed to the remote systems using a software distribution tool from an independent software vendor (ISV). When the package is distributed, the installation script executes to install the software.

Creating And Distributing The Typical Unattended Installation Package

The **Typical Setup** unattended installation option uses the *Dell EMC Systems Management Tools and Documentation* DVD as the unattended installation package. The `msiexec.exe /i <SysMgmtx64>.msi /qn` command accesses the DVD to accept the software license agreement and installs all the required Server Administrator features on selected remote systems. These features are installed on the remote systems based on the system's hardware configuration.

NOTE: After an unattended installation is complete, to use the command line interface (CLI) feature of Server Administrator, you must open a new console window and execute the CLI commands from there. Executing CLI commands from the same console window in which Server Administrator was installed does not work.

You can make the DVD image available to the remote system by either distributing the entire contents of the media, or by mapping a drive from the target system to the location of the DVD image.

Mapping A Drive To Act As The Typical Unattended Installation Package

1. Share an image of the *Systems Management Tools and Documentation* software with each remote system on which you want to install Server Administrator.

   You can accomplish this task by directly sharing the software or by copying the entire ISO image to a drive and sharing the copy.
2. Create a script that maps a drive from the remote systems to the shared drive described in step 1. This script should execute `msiexec.exe /i Mapped Drive\<64-bit MSI path on the DVD>/qn` after the drive has been mapped.
3. Configure the ISV distribution software to distribute and execute the script created in step 2.
4. Distribute this script to the target systems by using the ISV software distribution tools.

   The script executes to install Server Administrator on each remote system.
5. Reboot each remote system to enable Server Administrator.

Distributing The Entire DVD as The Typical Unattended Installation Package

1. Distribute the entire image of the *Systems Management Tools and Documentation* DVD to the target systems.
2. Configure the ISV distribution software to execute the `msiexec.exe /i DVD Drive\<64-bit MSI path on the DVD>/qn` command from the DVD image.

   The program executes to install Server Administrator on each remote system.
3. Reboot each remote system to enable Server Administrator.

Creating Custom Unattended Installation Packages

To create a custom unattended installation package, perform the following steps:

1. Copy the **SYSMGMT64\srvadmin\windows** directory from the DVD to the system hard drive.
2. Create a batch script that executes the installation using the Windows Installer Engine (**msiexec.exe**).

   NOTE: For Customized Unattended Installation, each required feature must be included as a command line interface (CLI) parameter for it to be installed.

   An example is `msiexec.exe /i SysMgmt64.msi ADDLOCAL= SA,IWS,BRCM /qn`.
3. Place the batch script in the **windows** directory on the system hard drive.

Related Links:

Customization Parameters

Distributing Custom Unattended Installation Packages

For distributing custom unattended installation packages:

1. Configure the ISV distribution software to execute the batch script once the installation package is distributed.
2. Use the ISV distribution software to distribute the custom unattended installation package to the remote systems. The batch script installs Server Administrator along with specified features on each remote system.

   The batch script installs Server Administrator along with specified features on each remote system.
3. Reboot each remote system to enable Server Administrator.

Specifying Log File Locations

For managed system MSI installation, run the following command to perform an unattended installation while specifying the log file location

```
msiexec.exe /i <SysMgmtx64>.msi /l*v
"C:\openmanage\logs\SysMgmt.log"
```

Unattended Installation Features

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.
- A prerequisite checker program that examines the dependency status of selected software features without having to perform an actual installation.

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 details about all the command-line switches for the Windows Installer Tools.

Table 5. Command Line Settings for MSI Installer

Setting	Result
`/i <Package|Product Code>`	This command installs or configures a product. **/i <SysMgmt or SysMgmtx64>.msi** – Installs the Server Administrator software.
`/i <SysMgmt or SysMgmtx64>.msi /qn`	This command carries out a fresh installation.
`/x <Package|Product Code>`	This command uninstalls a product. **/x <SysMgmt or SysMgmtx64>.msi** – Uninstalls the Server Administrator software. For the product GUID, see Unattended Uninstall Using The Product GUID
`/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 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 be reinstalled. **/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 this reinstall option for the first installation of an application or feature.
`INSTALLDIR=<path>`	This command installs a product in 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 without displaying an error message. **/i <SysMgmt or SysMgmtx64>.msi INSTALLDIR=c:\OpenManage /qn** – installs a product to a specific location where **c:\OpenManage** is the install location.
`CP_MESSAGE_FORMAT=<enhanced | traditional>`	This command sets the alert message type to **Enhanced Message Format** (recommended) or **Traditional Message Format**.

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 a silent or unattended installation. With the customization parameters, you 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.

You can include the **REINSTALL** customization parameter on the command line and assign the feature ID (IDs) of the software feature that you want to reinstall. For example, `msiexec.exe /i SysMgmt.msi REINSTALL=BRCM /qn`

This command runs the installation for Systems Management and reinstalls 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 (IDs) of the software feature that you want to uninstall. For example, `msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qn`

This command runs the installation for 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 /qn`

This command runs the installation for managed system software, and uninstalls the Broadcom agent. This execution is in an unattended but not silent mode.

The following table provides the list of feature IDs for each software feature.

NOTE: The software feature IDs mentioned in the table are case-sensitive.

Table 6. Software Feature IDs for Managed Systems Software

Feature ID	Description
ALL	All features
BRCM	Broadcom Network Interface Card (NIC) Agent
QLG	QLogic SNMP Agent
INTEL	Intel NIC Agent
IWS	Server Administrator Web Server
OMSS	Server Administrator Storage Management Service
RAC	iDRAC Command Line Tools
iDRAC (for 11th generation of PowerEdge servers)	Integrated DRAC Command Line Tools
iDRAC12G (for 12th generation of PowerEdge servers)	Integrated DRAC Command Line Tools
SI	Server Instrumentation
RmtMgmt	Remote Enablement
CLI	Command Line Interface of Server Instrumentation
WMI	Windows Management Instrumentation Interface of Server Instrumentation
SNMP	Simple Network Management Protocol Interface of Server Instrumentation
OSLOG	Operating System Logging
SA	Installs SI, CLI, WMI, SNMP, OSLOG

Feature ID	Description
OMSM	Installs SI, OMSS, CLI, WMI, SNMP, OSLOG

NOTE: To manage the server, select either Server Administrator Webserver or one of the Management Interfaces – CLI, WMI, SNMP or OSLOG along with Server Instrumentation (SI) or Server Administrator Storage Management Service (OMSS).

NOTE: If SI or OMSS is installed using silent installation (unattended installation), then IWS and WMI are automatically installed.

MSI Return Code

An application event log entry is recorded in the SysMgmt.log file. The following table shows some of the error codes returned by the msiexec.exe Windows Installer Engine.

Table 7. 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_SUCCESS_REBOOT_REQUIRED	3010	A restart is required to complete the installation. This message is indicative of a successful installation.

NOTE: For more information on all the error codes returned by the msiexec.exe and InstMsi.exe Windows Installer functions, see support.microsoft.com.

System Recovery On Failed Installation

The Microsoft Software Installer (MSI) provides the ability to return a system to its fully working condition after a failed installation. MSI does this by maintaining an undo operation for every standard action it performs during an install, upgrade, or uninstall. This operation includes restoration of deleted or overwritten files, registry keys, and other resources. Windows temporarily saves all files that it deletes or overwrites during the course of an installation or removal, so that they can be restored if necessary, which is a type of rollback. After a successful installation, Windows deletes all of the temporary backup files.

In addition to the rollback of MSI Standard Actions, the library also has the ability to undo commands listed in the INI file for each application if a rollback occurs. All files that are modified by the installation actions are restored to their original state if a rollback occurs.

When the MSI engine is going through the installation sequence, it ignores all actions that are scheduled as rollback actions. If a Custom Action, MSI Standard Action, or a installation action fails, then a rollback starts.

You cannot roll back an installation once it is completed; transacted installation is only intended as a safety net that protects the system during an installation session. If you want to remove an installed application, you should uninstall that application.

NOTE: Driver installation and removal is not executed as part of the installation transaction and therefore cannot be rolled back if a fatal error occurs during execution.

NOTE: Installations, uninstallations, and upgrades that you cancel during installer cleanup, or after the installation transaction is completed, are not rolled back.

Failed Updates

Apply the MSI patches and updates provided by vendors to the original vendor MSI packages provided. If you intentionally or accidentally repackage an MSI package, or make changes to it directly, patches and updates may fail. MSI packages must not be repackaged; doing so changes the feature structure and Globally Unique Identifier (GUID), which break any provided patches or updates. To make any changes to a vendor-provided MSI package, use a .mst transform file.

NOTE: A GUID is 128-bit long, and the algorithm used to generate a GUID guarantees unique GUID. The product GUID uniquely identifies the application.

Uninstalling Managed System Software

You can uninstall managed system software features by using the *Dell EMC OpenManage Systems Management Tools and Documentation* software, or the operating system. You can simultaneously perform unattended uninstallation on multiple systems.

Uninstalling Managed System Software Using The Provided Media

Perform the following tasks to uninstall managed system software using the provided media.

1. Insert the *Dell EMC OpenManage Systems Management Tools and Documentation* software into the system's DVD drive.
   If the setup program does not start automatically, run the **setup.exe** in the **SYSMGMT64\srvadmin\windows** directory on the DVD.
   The **Server Administrator prerequisite** status screen is displayed and runs the prerequisite checks for the managed system. Any relevant informational, warning, or error messages detected during checking are displayed. Resolve all error and warning situations, if any.
2. Click the **Install, Modify, Repair, or Remove Server Administrator** option.
   The **Welcome to the Install Wizard for Server Administrator** screen is displayed.
3. Click **Next**.
   This dialog enables you to modify, repair, or remove the program.
   The **Program Maintenance** dialog box is displayed.
4. Select the **Remove** option and click **Next**.
   The **Remove the Program** dialog box is displayed.
5. Click **Remove**.
   The **Uninstalling Server Administrator** screen is displayed and provides the status and progress of the software features being uninstalled.
   When the selected features are uninstalled, the **Install Wizard Completed** dialog box is displayed.
6. Click **Finish** to exit the Server Administrator uninstallation.
   If you are prompted to reboot the system, select from the following reboot options:
   - **Yes, reboot my system now**.
   - **No, I will reboot my system later**.

   All Server Administrator features are uninstalled.

Uninstalling Managed System Software Features Using The Operating System

Perform the following tasks to uninstall managed system software features using the operating system.

1. Navigate to the Windows **Control Panel**.
2. Click **Add/Remove Programs**.
3. Click **Server Administrator**, and then click **Remove**.
   The **Add or Remove Programs** dialog box is displayed.
4. Click **Yes** to confirm uninstallation of Server Administrator.
   The **Server Administrator** screen is displayed and provides the status and progress of the software features being uninstalled.

If you are prompted to reboot the system, select from the following reboot options:

- **Yes, reboot my system now**.
- **No, I will reboot my system later**

All Server Administrator features are uninstalled.

Unattended uninstall using the product GUID

If you do not have the installation image or the MSI package available during an uninstallation, use the package GUIDs in the command line to uninstall systems management software on managed systems or management stations running Windows operating system.

For managed systems, use `msiexec.exe /x {826996FB-E97F-44BE-BC09-7B2EAFDA739B}`

Unattended Uninstallation Of Managed System Software

The systems management installer features an unattended uninstallation procedure. Unattended uninstallation enables you to simultaneously uninstall managed systems software from multiple systems. The unattended uninstallation package is distributed to the remote systems using a software distribution tool from an ISV. When the package is distributed, the uninstallation script executes to uninstall the software.

Distributing The Unattended Uninstallation Package

The *Systems Management Tools and Documentation* software is pre-configured to act as the unattended uninstallation package. To distribute the package to one or more systems:

1. Configure the ISV distribution software to execute the `msiexec.exe /x DVD Drive\<64-bit MSI path on the DVD>/qb` command, if you are using the DVD, after the unattended uninstallation package has been distributed.
2. Use the ISV distribution software to distribute the typical unattended uninstallation package to the remote systems.

   The program executes to uninstall managed systems software on each remote system.
3. Reboot each remote system to complete uninstallation.

Unattended Uninstall Command Line Settings

The Command Line Settings for MSI Installer table shows the unattended uninstall command line settings available for unattended uninstallation. Type the optional settings on the command line after `msiexec.exe /x <SysMgmtx64>.msi` with a space between each setting.

For example, running `msiexec.exe /x SysMgmt.msi /qb` runs the unattended uninstallation, and displays the unattended uninstallation status while it is running.

Running `msiexec.exe /x <SysMgmtx64>.msi /qn` runs the unattended uninstallation, but silently (without displaying messages.)

4

Installing Managed System Software On Microsoft Windows Server and Microsoft Hyper-V Server

The Server Core installation option of the Microsoft Windows Server and Hyper-V Server operating system provides a minimal environment for running specific server roles that reduce the maintenance and management requirements and the attack surface for those server roles. A Windows Server or Hyper-V Server installation installs only a subset of the binaries that are required by the supported server roles. For example, the Explorer shell is not installed as part of a Windows Server or Hyper-V Server installation. Instead, the default user interface for a Windows Server or Hyper-V Server installation is the command prompt.

NOTE: On Windows client operating systems, to install the systems management software successfully, log in using an account which belongs to the Administrators group and must run the setup.exe using the option Run as administrator from the right-click menu.

NOTE: Log in as a built-in Administrator, Domain Administrator, or user who is a part of Domain Admins and Domain Users group, to install the systems management software on supported Microsoft Windows operating system. For more information about user privileges, see the corresponding Microsoft Windows operating system Help.

Running Prerequisite Checker In CLI Mode

You must run the prerequisite checker in the CLI mode as Windows Server and Hyper-V Server does not support the GUI mode.

Related Links:

Prerequisite Checker

Installing Managed System Software In CLI Mode

Launch the MSI file from the command prompt using the command `msiexec /i <SysMgmtx64>.msi`.

To install the localized version of the managed system software, type

```
msiexec /i <SysMgmtx64>.msi TRANSFORMS= <languauge_transform >.mst
```

in the command prompt. Replace **<language_transform >.mst** with the appropriate language file:

- **1031.mst** (German)
- **1034.mst** (Spanish)
- **1036.mst** (French)
- **1041.mst** (Japanese)
- **2052.mst** (Simplified Chinese)

Related Links:

Optional Command Line Settings

Uninstalling Systems Management Software

To uninstall managed system software, type `msiexec /x <SysMgmtx64>.msi` at the command prompt.

5

Using Microsoft Active Directory

If you use Active Directory service software, configure it to control access to the network. The Active Directory database is modified to support remote management authentication and authorization. Server Administrator, as well as Integrated Remote Access Controllers (iDRAC), Remote Access Controllers (RAC), can now interface with Active Directory. With this tool, you can add and control users and privileges from one central database.

Active Directory Schema Extensions

The Active Directory data exists in a distributed database of **Attributes** and **Classes**. An example of a Active Directory **Class** is the **User** class. Some example Attributes of the user class might be the user's first name, last name, phone number, and so on. Define every **Attribute** or **Class** that is added to an existing Active Directory schema with a unique ID. To maintain unique IDs throughout the industry, Microsoft maintains a database of Active Directory Object Identifiers (OIDs).

The Active Directory schema defines the rules for what data can be included in the database. To extend the schema in Active Directory, install the latest received unique OIDs, unique name extensions, and unique linked attribute IDs for the new attributes and classes in the directory service from the *Dell EMC OpenManage Systems Management Tools and Documentation* software.

Extension : dell

Base OID : 1.2.840.113556.1.8000.1280

Link ID range :12070 to 12079

Overview Of The Active Directory Schema Extensions

Customized classes, or groups of objects can be created and configured by the user to meet their unique needs. New classes in the schema include an Association, a Product, and a Privilege class. An association object links the user or group to a given set of privileges and to systems (Product Objects) in the network. This model gives an administrator control over the different combinations of user, privilege, and system or RAC device on the network, without adding complexity.

Active Directory Object Overview

For each of the systems that you want to integrate with Active Directory for authentication and authorization, there must be at least one Association Object and one Product Object. The Product Object represents the system. The Association Object links it with users and privileges. You can create as many Association Objects as you need.

Each Association Object can be linked to as many users, groups of users, and Product Objects as required. The users and Product Objects can be from any domain. However, each Association Object may only link to one Privilege Object. This behavior allows an administrator to control users and their rights on specific systems.

The Product Object links the system to Active Directory for authentication and authorization queries. When a system is added to the network, the administrator must configure the system and its product object with its Active Directory name so that users can perform authentication and authorization with Active Directory. The administrator must also add the system to at least one Association Object for users to authenticate.

The following figure illustrates that the Association Object provide the connection that is needed for all of the authentication and authorization.

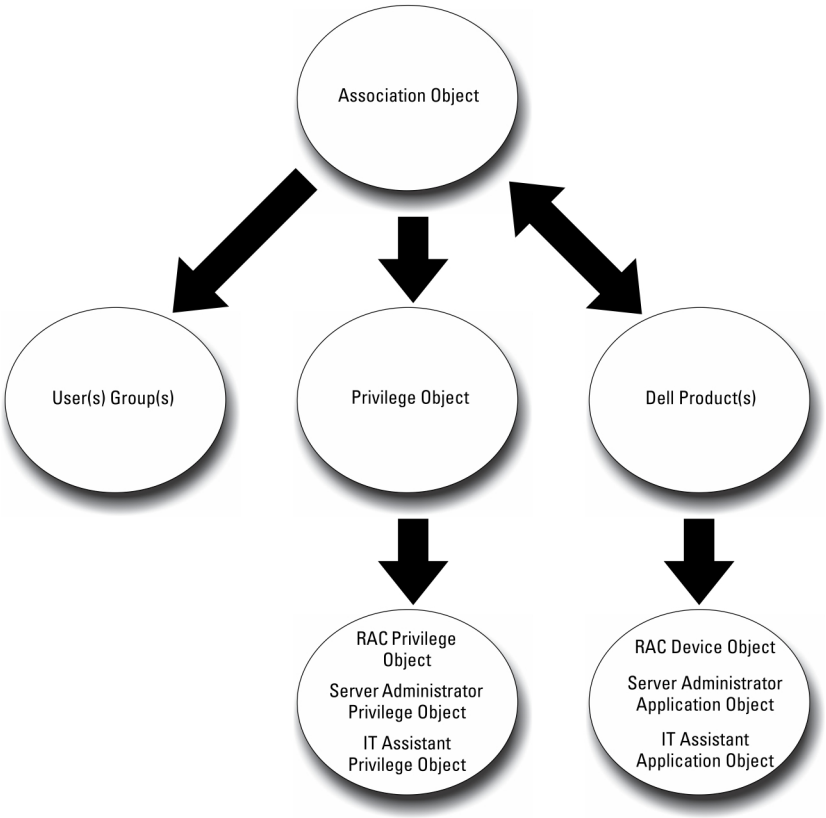

Figure 1. Typical Setup for Active Directory Objects

In addition, you can set up Active Directory objects in a single domain or in multiple domains. Setting up objects in a single domain does not vary, whether you are setting up RAC, or Server Administrator objects. When multiple domains are involved, however, there are some differences.

The following figure shows the set up of the Active Directory objects in a single domain. In this scenario, you have two DRAC 4 cards (RAC1 and RAC2) and three existing Active Directory users (User1, User2, and User3). You want to give User1 and User2 administrator privilege on both DRAC 4 cards and give User3 login privilege on the RAC2 card.

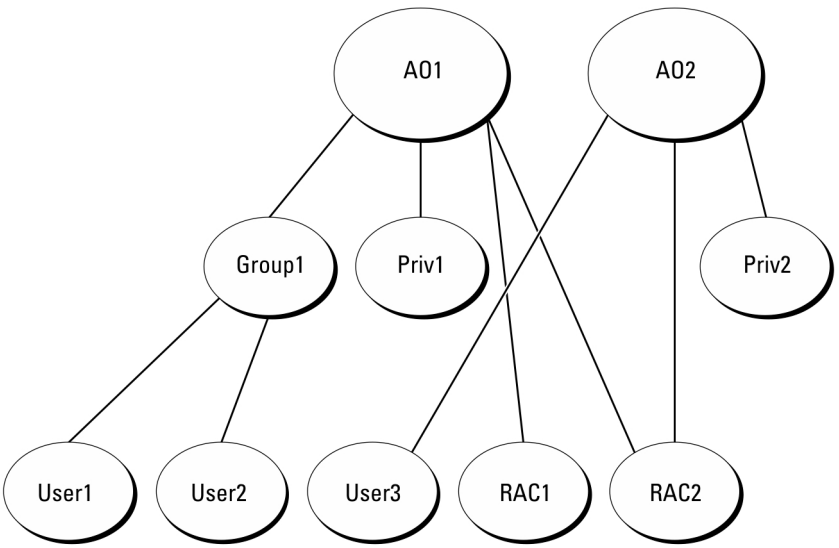

Figure 2. Setting Up RAC Active Directory Objects in a Single Domain

Setting Up Objects In A Single Domain

To set up the objects in a single domain scenario, perform the following tasks:

1. Create two Association Objects.
2. Create two RAC Product Objects, RAC1 and RAC2, to represent the two DRAC 4 cards.
3. Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (administrator) and Priv2 has login privileges.
4. Group User1 and User2 into Group1.
5. Add Group1 as Member in Association Object 1 (AO1), Priv1 as Privilege Object in AO1, and both RAC1 and RAC2 as RAC Products in AO1.
6. Add User3 as Member in Association Object 2 (AO2), Priv2 as Privilege Object in AO2, and RAC2 as RAC Product in AO2.

Related Links:

Adding Users and Privileges to Active Directory

Active Directory Objects In Multiple Domains

The following figure shows the setup of the Active Directory objects in multiple domains for RAC. In this scenario, you have two DRAC 4 cards (RAC1 and RAC2) and three existing Active Directory users (User1, User2, and User3). User1 is in Domain1, but User2 and User3 are in Domain2. You want to give User1 and User2 Administrator privileges on both the RAC1 and RAC2 card and give User3 Login privilege on the RAC2 card.

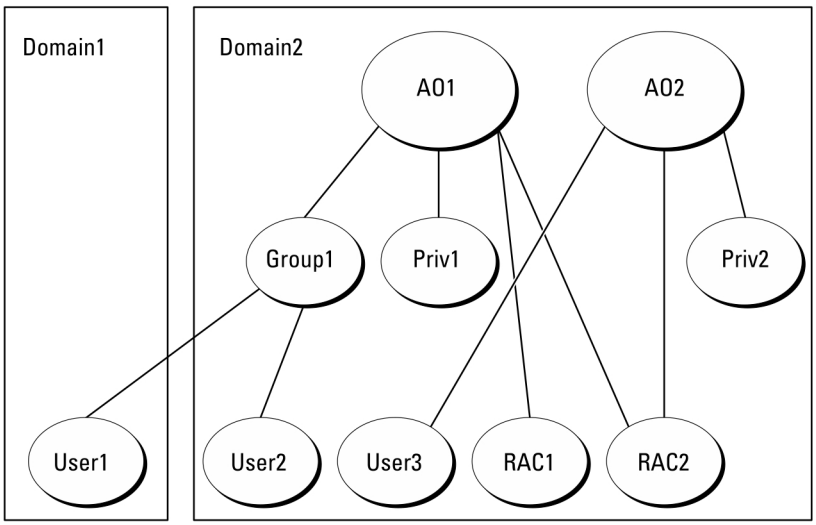

Figure 3. Setting Up RAC Active Directory Objects In Multiple Domains

Setting Up RAC Active Directory Objects In Multiple Domain

To set up the objects for this multiple domain scenario, perform the following tasks:

1. Ensure that the domain forest function is in Native mode.
2. Create two Association Objects, AO1 (of Universal scope) and AO2, in any domain.
3. Create two RAC Device Objects, RAC1 and RAC2, to represent the two remote systems.
4. Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (Administrator) and Priv2 has Login privileges.
5. Group User1 and User2 into Group1. The group scope of Group1 must be Universal.
6. Add Group1 as Member in Association Object 1 (AO1), Priv1 as Privilege Object in AO1, and both RAC1 and RAC2 as Products in AO1.
7. Add User3 as Member in Association Object 2 (AO2), Priv2 as Privilege Object in AO2, and RAC2 as a Product in AO2.

Setting Up Server Administrator Active Directory Objects In Multiple Domains

For Server Administrator, the users in a single Association can be in separate domains and need not be in a Universal group. The following is a very similar example to show how Server Administrator systems in separate domains affect the setup of directory objects. Instead of RAC devices, you will have two systems running Server Administrator (Server Administrator Products sys1 and sys2). sys1 and sys2 are in different domains. You can use any existing Users or Groups that you have in Active Directory. The following figure shows how to set up the Server Administrator Active Directory objects for this example.

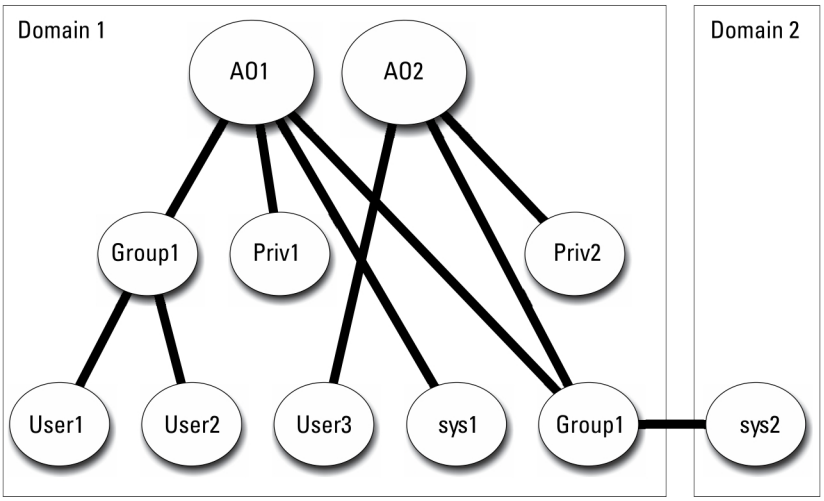

Figure 4. Setting up Server Administrator Active Directory Objects In Multiple Domains

Setting Up Server Administrator Active Directory Objects For Multiple Domain

To set up the objects for this multiple domain scenario, perform the following tasks:

1. Ensure that the domain forest function is in Native mode.
2. Create two Association Objects, AO1 and AO2, in any domain. The figure shows the objects in Domain1.
3. Create two Server Administrator Products, sys1 and sys2, to represent the two systems. sys1 is in Domain1 and sys2 is in Domain2.
4. Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (Administrator) and Priv2 has Login privileges.
5. Group sys2 into Group1. The group scope of Group1 must be **Universal**.
6. Add User1 and User2 as Members in Association Object 1 (AO1), Priv1 as Privilege Objects in AO1, and both sys1 and Group1 as Products in AO1.
7. Add User3 as a Member in Association Object 2 (AO2), Priv2 as a Privilege object in AO2, and Group1 as a Product in AO2.

NOTE: Neither of the Association objects needs to be of Universal scope.

Configuring Active Directory To Access The Systems

Before you can use Active Directory to access the systems, you must configure both the Active Directory software and the systems.

1. Extend the Active Directory schema.
2. Extend the Active Directory Users and Computers Snap-in.
3. Add system users and their privileges to Active Directory.
4. For RAC systems, enable SSL on each of the domain controllers.
5. Configure the system's Active Directory properties using either the Web-based interface or the CLI.

Related Links:

- Extending the Active Directory Schema
- Installing the Extension to the Active Directory Users and Computers Snap-In

- Adding Users and Privileges to Active Directory
- Configuring the Systems or Devices

Configuring The Active Directory Product Name

To configure the Active Directory product name:

1. Locate the **omsaoem.ini** file in the installation directory.
2. Edit the file to add the line `adproductname=text`, where `text` is the name of the product object that you created in Active Directory. For example, the **omsaoem.ini** file contains the following syntax if the Active Directory product name is configured to `omsaApp`.

```
productname=Server Administrator
startmenu=Dell OpenManage Applications
autdbid=omsa
accessmask=3
adsupport=true
adproductname=omsaApp
```

3. Restart the **Systems Management Server Administrator (DSM SA) Connection Service** after saving the **omsaoem.ini** file.

Extending The Active Directory Schema

The schema extensions for RAC and Server Administrator are available. Extend the schema for software or hardware that you are using. Apply each extension individually to receive the benefit of its software-specific settings. Extending the Active Directory schema adds schema classes and attributes, example privileges and association objects, and a organizational unit to the schema.

NOTE: Before you extend the schema, you must have *Schema Admin* privileges on the Schema Master Flexible Single Master Operation (FSMO) Role Owner of the domain forest.

Extend the schema using two different methods. Use the Schema Extender utility, or use the Lightweight Directory Interchange Format (LDIF) script file.

NOTE: The organizational unit is not added if you use the LDIF script file.

The LDIF script files and the Schema Extender utility are located in the following directories on the *Dell EMC OpenManage Systems Management Tools and Documentation* software:

- <DVD drive>drive>:\SYSMGMT64\ManagementStation\support\OMActiveDirect ory_Tools\<installation type>\LDIF Files
- <DVD drive>:\SYSMGMT64\ManagementStation\support\OMActiveDirect ory_ Tools\<installation type>\Schema Extender

The following table lists the folder names and *<installation type>*.

Table 8. Folder Names and Installation Types

Folder Name	Installation Type
OMSA	Server Administrator
Remote_Management	RAC 5, CMC, and iDRAC on xx0x Blade systems
Remote_Management_Advanced	iDRAC on xx1x and xx2x systems **NOTE: Only iDRAC6 is supported on xx1x systems and iDRAC7 is supported on xx2X systems.**

To use the LDIF files, see the instructions in the readme that is in the LDIF files directory. To use the Schema Extender to extend the Active Directory Schema, perform the steps in Using the Dell Schema Extender.

Copy and run the Schema Extender or LDIF files from any location.

Using The Dell Schema Extender

To use the Dell Schema Extender perform the following tasks:

CAUTION: The Dell Schema Extender uses the SchemaExtenderOem.ini file. To ensure that the Dell Schema Extender utility functions properly, do not modify the name or the contents of this file.

1. Click **Next** on the Welcome screen.
2. Read the warning and click **Next**.
3. Select **Use Current Log In Credentials** or enter a user name and password with schema administrator rights.
4. Click **Next** to run the Dell Schema Extender.
5. Click **Finish**.

   To verify the schema extension, use the Active Directory Schema Snap-in in the Microsoft Management Console (MMC) to verify the existence of the following classes and attributes. See the Microsoft documentation for more information on enabling and using the Active Directory Schema Snap-in.

   For more information on class definitions for DRAC, see the *Remote Access Controller 4 User's Guide and Remote Access Controller 5 User's Guide*. For more information on class definitions for iDRAC, see the *Integrated Remote Access Controller User's Guide*.

Table 9. Class Definitions for Classes Added to the Active Directory Schema

Class Name	Assigned Object Identification Number (OID)	Class Type
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2	Structural Class
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4	Structural Class
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5	Structural Class
dellOmsa2AuxClass	1.2.840.113556.1.8000.1280.1.2.1.1	Auxiliary Class
dellOmsaApplication	1.2.840.113556.1.8000.1280.1.2.1.2	Structural Class

Table 10. dellAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Description	This class represents the Association Object. The Association Object provides the connection between the users and the devices or products.
Class Type	Structural Class
SuperClasses	Group
Attributes	dellProductMembers dellPrivilegeMember

Table 11. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Description	This class is used as a container Class for the Privileges (Authorization Rights).
Class Type	Structural Class
SuperClasses	User
Attributes	dellRAC4Privileges dellRAC3Privileges dellOmsaAuxClass

Table 12. dellProduct Class

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Description	This is the main class from which all the products are derived.
Class Type	Structural Class
SuperClasses	Computer
Attributes	dellAssociationMembers

Table 13. dellOmsa2AuxClass Class

OID	1.2.840.113556.1.8000.1280.1.2.1.1
Description	This class is used to define the privileges (Authorization Rights) for Server Administrator.
Class Type	Auxiliary Class
SuperClasses	None
Attributes	dellOmsaIsReadOnlyUser dellOmsaIsReadWriteUser dellOmsaIsAdminUser

Table 14. dellOmsaApplication Class

OID	1.2.840.113556.1.8000.1280.1.2.1.2
Description	This class represents the Server Administrator application. Server Administrator must be configured as dellOmsaApplication in Active Directory. This configuration enables the Server Administrator application to send LDAP queries to Active Directory.
Class Type	Structural Class
SuperClasses	dellProduct
Attributes	dellAssociationMembers

Table 15. General Attributes Added to the Active Directory Schema

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellPrivilegeMember List of dellPrivilege Objects that belong to this Attribute.	1.2.840.113556.1.8000.1280.1.1.2.1 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers List of dellRacDevices Objects that belong to this role. This attribute is the forward link to the dellAssociationMembers backward link. Link ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellAssociationMembers List of dellAssociationObjectMembers that belong to this Product. This attribute is the backward link to the dellProductMembers Linked attribute.	1.2.840.113556.1.8000.1280.1.1.2.14 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
Link ID: 12071		

Table 16. Server Administrator-Specific Attributes Added to the Active Directory Schema

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellOMSAIsReadOnlyUser TRUE if the User has Read-Only rights in Server Administrator	1.2.840.113556.1.8000.1280.1.2.2.1 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellOMSAIsReadWriteUser TRUE if the User has Read-Write rights in Server Administrator	1.2.840.113556.1.8000.1280.1.2.2.2 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellOMSAIsAdminUser TRUE if the User has Administrator rights in Server Administrator	1.2.840.113556.1.8000.1280.1.2.2.3 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

Active Directory Users And Computers Snap-In

When you extend the schema in Active Directory, extend the Active Directory Users and Computers snap-in so that the administrator can manage Products, Users and User Groups, Associations, and Privileges. Extend the snap-in once, even if you have added more than one schema extension. Install the snap-in on each system that you intend to use for managing these objects.

Installing The Extension To The Active Directory Users And Computers Snap-In

When you are installing the systems management software using the *Systems Management Tools and Documentation* DVD, you can install the Snap-in by selecting the **Active Directory Snap-in** option.

For 64-bit Windows operating systems, the Snap-in installer is located under `<DVD drive>:\SYSMGMT\x64\ManagementStation\windows\ADSnapIn`.

NOTE: Install the Administrator Pack on each management station that is managing the new Active Directory objects. If you do not install the Administrator Pack, you cannot view the new object in the container.

NOTE: For more information about the Active Directory Users and Computers snap-in, see the Microsoft documentation.

Related Links:

Opening the Active Directory Users and Computers Snap-In

Opening The Active Directory Users And Computers Snap-In

To open the Active Directory Users and Computers snap-in, perform the following steps:

1. If you are on the domain controller, click **Start** → **Admin Tools** → **Active Directory Users and Computers**. If you are not on the domain controller, you must have the appropriate Microsoft administrator pack installed on the local system. To install this administrator pack, click **Start** → **Run**, type `MMC`, and press <**Enter**>.
2. Click **File** in the **Console 1** window.
3. Click **Add/Remove Snap-in**.
4. Click **Add**.
5. Select the **Active Directory Users and Computers** snap-in and click **Add**.
6. Click **Close** and click **OK**.

Adding Users And Privileges To Active Directory

The extended Active Directory Users and Computers snap-in allows you to add DRAC and Server Administrator users and privileges by creating RAC, Association, and Privilege objects. To add an object, perform the steps in the applicable subsection.

Creating A Product Object

To create a Product Object:

NOTE: Server Administrator users must use Universal-type Product Groups to span domains with their product objects.

NOTE: When adding Universal-type Product Groups from separate domains, create an Association object with Universal scope. The default Association objects created by the Schema Extender utility are domain Local Groups and do not work with Universal-type Product Groups from other domains.

1. In the **Console Root** (MMC) window, right-click a container.
2. Select **New**.
3. Select a RAC or Server Administrator object, depending on what you have installed.

   The **New Object** window is displayed.
4. Type in a name for the new object. This name must match the **Active Directory product name** as discussed in Configuring Active Directory Using CLI on Systems Running Server Administrator.
5. Select the appropriate **Product Object**.
6. Click **OK**.

Creating A Privilege Object

Privilege Objects must be created in the same domain as the Association Object to which they are associated.

1. In the **Console Root** (MMC) window, right-click a container.
2. Select **New**.
3. Select a RAC or Server Administrator object, depending on what you have installed.

   The **New Object** window is displayed.
4. Type in a name for the new object.
5. Select the appropriate **Privilege Object**.
6. Click **OK**.
7. Right-click the privilege object that you created and select **Properties**.
8. Click the appropriate **Privileges** tab and select the privileges that you want the user to have.

Creating An Association Object

The Association Object is derived from a Group and must contain a group Type. The Association Scope specifies the Security Group Type for the Association Object. When you create an Association Object, choose the Association Scope that applies to the type of objects you intend to add. Selecting Universal, for example, means that Association Objects are only available when the Active Directory Domain is functioning in Native Mode.

1. In the **Console Root** (MMC) window, right-click a container.
2. Select **New**.
3. Select a RAC or Server Administrator object, depending on what you have installed.

   The **New Object** window is displayed.
4. Type in a name for the new object.
5. Select **Association Object**.
6. Select the scope for the **Association Object**.
7. Click **OK**.

Adding Objects To An Association Object

By using the **Association Object Properties** window, you can associate users or user groups, privilege objects, systems, RAC devices, and system or device groups.

NOTE: RAC users must use Universal Groups to span domains with their users or RAC objects.

You can add groups of Users and Products. You can create related groups in the same way that you created other groups.

To Add Users Or User Groups

1. Right-click the **Association Object** and select **Properties**.
2. Select the **Users** tab and click **Add**.
3. Type the User or User Group name or browse to select and click **OK**.

Click the **Privilege Object** tab to add the privilege object to the association that defines the user's or user group's privileges when authenticating to a system.

NOTE: Add only one Privilege Object to an Association Object.

To Add A Privilege

1. Select the **Privileges Object** tab and click **Add**.
2. Type the Privilege Object name or browse and click **OK**.

   Click the **Products** tab to add one or more systems or devices to the association. The associated objects specify the products connected to the network that are available for the defined users or user groups.

NOTE: Add multiple systems or RAC devices to an Association Object.

To Add Products

1. Select the **Products** tab and click **Add**.
2. Type the system, device, or group name and click **OK**.
3. In the **Properties** window, click **Apply** and then **OK**.

Configuring The Systems Or Devices

For instructions on configuring the Server Administrator systems using CLI commands, see Configuring Active Directory Using CLI on Systems Running Server Administrator. For DRAC users, see the *Remote Access Controller User's Guide* or *Remote Access Controller User's Guide*. For iDRAC users, see the *Integrated Remote Access Controller User's Guide*.

NOTE: The systems on which Server Administrator is installed must be a part of the Active Directory domain and should also have computer accounts on the domain.

Configuring Active Directory Using CLI On Systems Running Server Administrator

You can use the `omconfig preferences dirservice` command to configure the Active Directory service. The **productoem.ini** file is modified to reflect these changes. If the **adproductname** is not present in the **productoem.ini** file, a default name is assigned.

The default value is **system name-software-product name**, where **system name** is the name of the system running Server Administrator, and **softwareproduct name** refers to the name of the software product defined in **omprv64.ini** (that is, **computerName-omsa**).

NOTE: This command is applicable only on Windows.

NOTE: Restart the Server Administrator service after you have configured Active Directory.

The following table shows the valid parameters for the command.

Table 17. Active Directory Service Configuration Parameters

name=value pair	Description
prodname=<text>	Specifies the software product to which you want to apply the Active Directory configuration changes. Prodname refers to the name of the product defined in **omprv64.ini**. For Server Administrator, it is omsa.
enable=<true | false>	**true**: Enables Active Directory service authentication support. **false**: Disables Active Directory service authentication support.
adprodname=<text>	Specifies the name of the product as defined in the Active Directory service. This name links the product with the Active Directory privilege data for user authentication.

6

Frequently Asked Questions

What ports do systems management applications use?

The default port used by Server Administrator is 1311. These ports are configurable. For port information of a particular component, see the User Guide of that respective component.

When I run virtual media on the iDRAC controller over a Wide Area Network (WAN) with low bandwidth and latency, launching Systems Management Install directly on the virtual media failed, what do I do?

Copy the web install package to the local system and then launch systems management Install.

Do I need to uninstall the Adaptec Fast Console application installed on the system before installing the Server Administrator Storage Management Service?

Yes, if you already have Adaptec Fast Console installed on the system, you must uninstall this application before installing the Server Administrator Storage Management Service.

Microsoft Windows

How do I fix a faulty installation of Server Administrator?

You can fix a faulty installation by forcing a reinstall and then performing an uninstall of Server Administrator. To force a reinstall:

1. Find out the version of Server Administrator that was previously installed.
2. Download the installation package for that version.
3. Locate **<SysMgmtx64>.msi** and enter the following command at the command prompt to force a reinstall.

   ```
   msiexec /i <SysMgmtx64>.msi REINSTALL=ALL REINSTALLMODE=vomus
   ```
4. Select **Custom Setup** and choose all the features that were originally installed. If you are not sure which features were installed, select all of them and perform the installation.

   NOTE: If you installed Server Administrator in a non-default directory, make sure to change it in Custom Setup as well.

Once the application is installed, you can uninstall it from **Add/Remove Programs**.

What do I do when the creation of WinRM listener fails with the following error message?

```
The CertificateThumbprint property must be empty when the SSL configuration will be shared
with another service
```

This error occurs when the Internet Information Server (IIS) is already installed and configured for HTTPS communication. Details about coexistence of IIS and WinRM is available at **technet.microsoft.com/en-us/library/cc782312.aspx**.

In this case, use the following command to create a HTTPS Listener with the **CertificateThumbprint** empty:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS
@{Hostname="<host_name>";CertificateThumbprint=""}
```

What are the firewall-related configuration that needs to be done for WinRM?

With firewall turned ON, WinRM must be added to the firewall exclusion list to allow TCP port 443 for HTTPS traffic.

When launching the Systems Management Install, an error message may display, stating a failure to load a specific library, a denial of access, or an initialization error. An example of installation failure during Systems Management Install is "failed to load OMIL64.DLL." What do I do?

This is most likely due to insufficient Component Object Model (COM) permissions on the system. To remedy this situation, see the article **support.installshield.com/kb/view.asp?articleid=Q104986**

The Systems Management Install 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
```

I get a misleading warning or error message during systems management installation.

If you have insufficient disk space on the Windows system drive, you may encounter misleading warning or error messages when you run systems management Install. Additionally, windows installer requires space to temporarily extract the installer package to the %TEMP% folder. Ensure that you have sufficient disk space (100 MB or more) on the system drive prior to running systems management Install.

I am getting the following error message while launching systems management Install:

```
An older version of Server Administrator software is detected on this system. You must
uninstall all previous versions of Server Administrator applications before installing this
version
```

If you see this error when trying to launch systems management Install, it is recommended that you run the **OMClean.exe** program, under the **SYSMGMT\srvadmin\support\OMClean** directory, to remove an older version of Server Administrator on the system.

When I run systems management Install, I see unreadable characters on the Prerequisite check information screen.

When you run systems management Install in English, German, French, or Spanish and get unreadable characters on the **Prerequisite Check Information** screen, ensure that the browser encoding has the default character set. Resetting the browser encoding to use the default character set resolves the problem.

Where can I find the MSI log files?

By default, the MSI log files are stored in the path defined by the **%TEMP%** environment variable.

I downloaded the Server Administrator files for Windows from the Support website and copied it to my own media. When I tried to launch the SysMgmt.msi file, it failed. What is wrong?

MSI requires all installers to specify the **MEDIAPACKAGEPATH** property if the MSI file does not reside on the root of the DVD.

This property is set to **SYSMGMT\srvadmin\windows\SystemsManagement** for the managed system software MSI package. If you want to make the own DVD you must ensure that the DVD layout stays the same. The **SysMgmt.msi** file must be located in the **SYSMGMT \srvadmin\windows\SystemsManagement**. For more detailed information, go to **msdn.microsoft.com** and search for

```
MEDIAPACKAGEPATH Property
```

Does systems management Install support Windows Advertised installation?

No. Systems management Install does not support Windows Advertised installation - the process of automatically distributing a program to client computers for installation, through the Windows group policies.

How do I check the disk space availability during custom installation?

In the **Custom Setup** screen, you must click an active feature to view the hard drive space availability or to change the installation directory. For example, if Feature A is selected for installation (active) and Feature B is not active, the **Change** and **Space** buttons are disabled if you click Feature B. Click Feature A to view the space availability or to change the installation directory.

What do I do when I see the current version is already installed message is displayed?

If you upgrade from version **X** to version **Y** using MSP and then try to use the version **Y** DVD (full install), the prerequisite checker on the version **Y** DVD informs you that the current version is already installed. If you proceed, the installation does not run in **Maintenance** mode and you do not get the option to **Modify**, **Repair**, or **Remove**. Proceeding with the installation removes the MSP and creates a cache of the MSI file present in the version **Y** package. When you run it a second time, the installer runs in **Maintenance** mode.

What is the best way to use the prerequisite checker information?

The prerequisite checker is available for Windows. See the readme file at **SYSMGMT\srvadmin\windows\PreReqChecker \readme.txt** on the *Systems Management Tools and Documentation* software, for detailed information about using the prerequisite checker.

In the Prerequisite Checker screen, I get the following message. What can I do to resolve this problem?

```
An error occurred while attempting to execute a Visual Basic Script. Please confirm that
Visual Basic files are installed correctly.
```

This error occurs when the prerequisite checker calls the systems management script, **vbstest.vbs** (a Visual Basic script), to verify the installation environment, and the script fails. The possible causes are:

- Incorrect Internet Explorer Security Settings.

  Ensure that **Tools** → **Internet Options** → **Security** → **Custom level** → **Scripting** → **Active scripting** is set to **Enable**.

  Ensure that **Tools** → **Internet Options** → **Security** → **Custom level** → **Scripting** → **Scripting of Java applets** is set to **Enable**.
- Windows Scripting Host (WSH) has disabled the running of VBS scripts. WSH is installed during operating system installation, by default. On Windows 2003, WSH can be configured to prevent the running of scripts with a **.VBS** extension.

  a. Right-click **My Computer** on the desktop and click **Open** → **Tools** → **Folder Options** → **File Types**.

  b. Look for the **VBS** file extension and ensure that **File Types** is set to **VBScript Script File**.

  c. If not, click **Change** and choose **Microsoft Windows Based Script Host** as the application that gets invoked to run the script.
- WSH is the wrong version, corrupted, or not installed. WSH is installed during operating system installation, by default. Download WSH from **msdn.microsoft.com**.

Is the time shown during installation or uninstallation by Windows Installer Services accurate?

No. During installation or uninstallation, the Windows Installer Service may display the time remaining for the current task to complete. This is only an approximation by the Windows Installer Engine based on varying factors.

Can I launch my installation without running the prerequisite checker? How do I do that?

Yes, you can. For example, you can run the MSI of the managed system software, directly from SYSMGMT\srvadmin\Windows \SystemsManagement. In general, it is not a good idea to bypass the prerequisite checker as there could be important information that you would not know otherwise.

How do I know what version of systems management software is installed on the system?

Navigate to the Windows **Control Panel** and double-click **Add/Remove Programs** and select **systems management software**. Select the link for **support information**.

Where can I see the Server Administrator features that are currently installed on my system?

Navigate to the Windows **Control Panel** and double-click **Add/Remove Programs** to view the Server Administrator features that are currently installed.

What are the names of all the systems management features under Windows?

The following table lists the names of all systems management features and their corresponding names in Windows.

Table 18. Systems Management Features — Windows

Feature	Name in WIndows
Managed System Services	
Server Administrator Instrumentation Service	DSM SA Data Manager DSM SA Event Manager
Server Administrator	DSM SA Connection Service DSM SA Shared Services (Disabled by default)