

Microsoft System Center 2012 R2

Deploying System Center 2012 - Operations Manager

Microsoft Corporation

Published: November 1, 2013

Authors

Byron Ricks

Applies To

System Center 2012 – Operations Manager

System Center 2012 Service Pack 1 (SP1) – Operations Manager

System Center 2012 R2 Operations Manager

Feedback

Send suggestions and comments about this document to sc2012docs@microsoft.com.

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2013 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Bing, Internet Explorer, JScript, SharePoint, Silverlight, SQL Server, Visio, Visual Basic, Visual Studio, Win32, Windows, Windows Intune, Windows PowerShell, and Windows Vista are trademarks of the Microsoft group of companies. Portions of this documentation related to network monitoring are provided by EMC, and for those portions the following copyright notice applies 2010 © EMC Corporation. All rights reserved. All other trademarks are property of their respective owners.

Revision History

Release Date	Changes
October 17, 2013	Original release of this guide.
November 1, 2013	Minor updates for this guide.

Contents

About This Document	7
Deploying System Center 2012 - Operations Manager.....	7
Planning the System Center 2012 - Operations Manager Deployment.....	8
Considerations when Upgrading to System Center 2012 - Operations Manager	9
Considerations for a Clean Installation of System Center 2012 – Operations Manager	11
Considerations when Designing a Management Group for Network Monitoring	12
Considerations for Application Performance Monitoring	14
Considerations for High Availability and Disaster Recovery.....	15
Deploying System Center 2012 - Operations Manager	15
Environmental Prerequisites for Operations Manager.....	19
Supporting Infrastructure	20
Security Considerations	21
Agent and Agentless Monitoring	29
Single-Server Deployment of Operations Manager.....	30
Walkthrough: Installing Operations Manager on a Single Server	33
Distributed Deployment of Operations Manager	38
How to Install the First Management Server in a Management Group	42
How to Install Additional Management Servers	46
How to Install the Operations Console	49
How to Configure the Operations Console to Use SSL When Connecting to a Reporting Server.....	50
How to Install the Operations Manager Web Console	51
Web Console Security in Operations Manager	55
How to Use FIPS Compliant Algorithms.....	56
How to Install the Operations Manager Reporting Server.....	58
Deploying a Gateway Server.....	61
How to Deploy a Gateway Server.....	62
How to Chain Gateways	66
Authentication and Data Encryption for Windows Computers.....	67
How to Obtain a Certificate Using Windows Server 2008 Enterprise CA	72
How to Obtain a Certificate Using Windows Server 2008 Stand-Alone CA	76
How to Configure an HTTPS Binding for a Windows Server 2008 CA	81
Deploying ACS and ACS Reporting.....	81
How to Install Audit Collection Services (ACS).....	83
How to Install an Audit Collection Services (ACS) Collector and Database.....	84
How to Deploy ACS on a Secondary Management Server	86
How to Deploy ACS Reporting.....	87
How to Deploy Audit Collection Services for UNIX/Linux	88

Using SQL Server 2012 Always On Availability Groups with System Center 2012 SP1 - Operations Manager	91
How to Upgrade from the Evaluation Version of Operations Manager	95
Installing Operations Manager by Using the Command Prompt Window	96
How to Enable High Availability for the Data Access Service	99
Using a Firewall	100
How to Configure the Operations Manager Database to Listen on a Specific TCP/IP Port	104
How to Configure the Reporting Data Warehouse to Listen on a Specific TCP/IP Port ...	106
Upgrading to System Center 2012 - Operations Manager.....	108
Upgrading from System Center Operations Manager 2007 R2	109
Upgrade Process Flow Diagrams.....	111
Upgrade Path Checklists for Operations Manager.....	113
Checklist: Single-Server Upgrade (Simple)	114
Checklist: Single-Server Upgrade (Complex)	116
Checklist: Distributed Upgrade (Simple)	119
Checklist: Distributed Upgrade (Complex).....	122
Pre-Upgrade Tasks for Operations Manager	129
Upgrade Tasks for Operations Manager	137
Improving Upgrade Performance	139
Upgrade Helper Management Pack.....	140
Upgrading Hardware and Software to Meet System Requirements	143
How to Add an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade).....	144
How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)	145
How to Replace an Operations Manager 2007 R2 Gateway that Has an Unsupported Configuration (Operations Manager Upgrade)	149
How to Remove an Operations Manager 2007 R2 Gateway (Operations Manager Upgrade).....	152
Upgrading SQL Server (Operations Manager Upgrade)	153
Upgrading a Single-Server Operations Manager 2007 R2 Environment	153
How to Upgrade an Operations Manager 2007 R2 Single-Server Management Group	154
Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group	157
Upgrading a Distributed Operations Manager 2007 R2 Environment.....	158
How to Upgrade a Secondary Management Server from Operations Manager 2007 R2	159
How to Upgrade a Gateway Server from Operations Manager 2007 R2	160
Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group	161
How to Upgrade Agents from Operations Manager 2007 R2	162
How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS..	167

How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server	169
Upgrading or Installing Optional Features	173
How to Upgrade a Stand-Alone Operations Console from Operations Manager 2007 R2	173
How to Upgrade a Web Console from Operations Manager 2007 R2	175
How to Upgrade Reporting from Operations Manager 2007 R2	176
How to Upgrade an ACS Collector from Operations Manager 2007 R2	178
Post-Upgrade Tasks when Upgrading from Operations Manager 2007 R2	179
Upgrading to System Center 2012 - Operations Manager by Using the Command Prompt Window.....	187
Maintaining the System Center 2012 - Operations Manager Infrastructure	189
Backup and Disaster Recovery in Operations Manager	190
Complete and Incremental Backups in Operations Manager	190
Backup File Naming Conventions in System Center 2012 - Operations Manager	192
Back Up System Center 2012 - Operations Manager.....	192
Recommended Backup Schedule for System Center 2012 - Operations Manager	193
How to Back Up Custom Management Packs.....	194
How to Schedule Backups of System Center 2012 - Operations Manager Databases	194
Backup and Recovery Using VSS Writer.....	197
Disaster Recovery in System Center 2012 - Operations Manager	197
Disaster Recovery Command-line Parameters.....	200
How to Restore Operations Manager Databases	202
Making Changes to an Operations Manager Environment	203
Account Information for Operations Manager	204
How to Change the Credentials for the Action Account.....	209
How to Change Credentials for the System Center Management Configuration service and System Center Data Access service	209
How to Change IIS ReportServer Application Pool Account Password	210
How to Change the Reporting Server Execution Account Password	211
How to Change the Windows Service Account Password for the SQL Server Reporting Service	211
How to Change the Run As Account Associated with a Run As Profile	212
How to Uninstall Operations Manager.....	213
How to Manage the Report Server Unattended Execution Account	213
How to Configure the Internet Proxy Settings for a Management Server	214
How to Move the Operational Database	214
How to Move the Data Warehouse Database	217
How to Move the Audit Collection Database	221
How to Move the Reporting Server Role.....	222
How to Remove the Management Server Role.....	224
Removing a Gateway Server from a Management Group	227
How to Remove Certificates Imported with MOMCertImport	230

Sending Data to Microsoft	231
Customer Experience Improvement Program (CEIP)	231
Operational Data Reporting (ODR)	232
Error Reporting	234

About This Document

The content in this guide is written primarily for online presentation in the [TechNet Library](#). The document version of this guide (.doc or .pdf) compiles the online topics into a single file. Because the individual online topics must include the appropriate context and navigation to other topics, you will note some redundancy between topics in the document version of this guide.

Document History

Release date	Changes
April 1, 2012	Original release of this guide.
January 15, 2013	Release for System Center 2012 Service Pack 1 (SP1) – Operations Manager

Deploying System Center 2012 - Operations Manager

The Deployment Guide contains information to help you:

1. Plan for and deploy System Center 2012 – Operations Manager
2. Plan for and deploy System Center 2012 Service Pack 1 (SP1), Operations Manager
3. Upgrade from Operations Manager 2007 R2
4. Maintain the Operations Manager infrastructure

Deploying Operations Manager consists of several phases, such as a design phase, testing phase, and a deployment phase. If you already have Operations Manager 2007 R2 implemented and want to move to System Center 2012 – Operations Manager, or have System Center 2012 – Operations Manager implemented and you want to move to System Center 2012 Service Pack 1 (SP1), you will go through several phases of upgrade, depending on your current topology. After you upgrade or deploy the product directly, you might want to make changes to your Operations Manager environment.

Tasks

The following topics introduce the task areas covered in the Deployment Guide:

- [Planning the System Center 2012 - Operations Manager Deployment](#)
- [Deploying System Center 2012 - Operations Manager](#)

- [Upgrading to System Center 2012 - Operations Manager](#)
- [Maintaining the System Center 2012 - Operations Manager Infrastructure](#)

For upgrade procedures to System Center 2012 Service Pack 1 (SP1), see the guide **Upgrading System Center 2012 – Operations Manager to System Center 2012 SP1**.

Downloadable Documentation

You can download a [copy of this technical documentation from the Microsoft Download Center](#). Always use the TechNet library for the most up-to-date information.

Planning the System Center 2012 - Operations Manager Deployment

This section provides information on major concepts to consider in the design and planning phase. This document provides high level scenarios, and points to details found throughout the [Deployment Guide for System Center 2012 – Operations Manager](#) as well as the [Operations Manager Sizing Helper](#) and specific concepts and procedures found in the [Operations Guide for System Center 2012 – Operations Manager](#).

Before You Begin

Before deploying, there are several sources of information you should read that are helpful for gaining context about Operations Manager functionality and requirements:

- **Getting Started**
Provides a learning roadmap intended for the operator in a Tier I role
- **Supported Configurations for System Center 2012 – Operations Manager**
Provides information about the supported operating systems, hardware configurations, software requirements, installation combinations, and security configurations - This document focuses on the system requirements and only mentions unsupported configurations when necessary

Designing and Planning for Deployment Scenarios

This document contains the following sections:

- [Considerations when Upgrading to System Center 2012 - Operations Manager](#)
Covers key concepts and considerations for upgrading to System Center 2012 – Operations Manager
- [Considerations for a Clean Installation of System Center 2012 – Operations Manager](#)
Covers key concepts and common configurations for a new, clean installation of System Center 2012 – Operations Manager
- [Considerations when Designing a Management Group for Network Monitoring](#)

Covers key concepts and considerations for discovering and monitoring network routers and switches, including the network interfaces and ports on those devices and the virtual LAN (VLAN) that they participate in

- [Considerations for Application Performance Monitoring](#)

Covers key concepts and considerations for monitoring Internet Information Services (IIS)-hosted .NET applications from server- and client-side perspectives in getting details about application performance and reliability that can help you pinpoint root causes of incidents

- [Considerations for High Availability and Disaster Recovery](#)

Covers key concepts to consider when designing for disaster recovery

Considerations when Upgrading to System Center 2012 - Operations Manager

This section of the Design and Planning material covers key concepts and considerations for upgrading to System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager. Complete upgrade scenarios and procedures are found in [Upgrading to System Center 2012 - Operations Manager](#).

The supported upgrade path is from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager, and then to System Center 2012 Service Pack 1 (SP1), so customers may have to perform multiple upgrades. Considerations when performing multiple upgrades include system requirements that do or do not overlap between System Center 2012 – Operations Manager and SP1. For example, you will want to consider what versions of SQL Server are supported and how moving across versions of SQL Server will be required as you upgrade across versions of Operations Manager.

If you have not reviewed **Getting Started** or **System Center 2012 - Operations Manager Supported Configurations**, you may want to before continuing. These documents contain key concepts and important configuration details you will find helpful as an upgrading customer.



Note

Unified Installer is a utility designed to perform new, clean installations of System Center 2012 for testing and evaluation purposes only. If you want to upgrade from an existing System Center installation or choose any set up options such as high availability or multi-server component installs, we recommend you refer instead to the procedures detailed in the deployment guides for each individual System Center 2012 component.

RMS Removal and the New RMS Emulator

In Operations Manager, the single largest change impacting design and planning is the removal of the root management server (RMS). All management servers are peers now that there is no RMS. Therefore, the RMS is no longer a single point of failure as all management servers host the services previously hosted only by the RMS. Roles are distributed to all the management servers. If one management server becomes unavailable, its responsibilities are automatically redistributed. An RMS emulator role provides for backwards compatibility for management packs

targeting the RMS. If you do not have any management packs that previously targeted the RMS, you will not need to make use of the RMS Emulator.

Preparing for Upgrade

Before upgrade:

Important

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

In a distributed management group upgrade, you upgrade the secondary management servers, the gateways, and agents. The order of agent upgrade depends on how the agents were deployed. If you installed the agents manually, you upgrade the agents before you upgrade the management servers and gateways.

1. Remove Agents from Pending Management
2. Check the Operations Manager 2007 R2 RMS for Active Connected Console
3. Disable Notification Subscription
4. Stop the Connector Services or Disable any Connector

These procedures are outlined in detail in [Pre-Upgrade Tasks for Operations Manager](#)

AD Integration and Agents

If you have any agents reporting to the RMS, move them to secondary management servers to take the agent work. It is important to manually upgrade your agents first. These procedures are outlined in detail in [Checklist: Distributed Upgrade \(Complex\)](#)

Data Warehouse

Data warehouse is now required; this is new for System Center 2012 – Operations Manager and is included in all sizing scenarios in the [Operations Manager Sizing Helper](#)

While upgrading, the UI will direct you to add a data warehouse if one does not exist.

Resource Pools

A resource pool is a collection of management servers, or gateway servers, used to distribute work amongst themselves and take over work from a failed member.

Due to the introduction of resource pools, we recommend that all management servers be connected by a low latency network. This means that if you are currently using management servers in multiple datacenters or sites we recommend you move all management servers to a single data center and use gateway servers at the other sites.

You should always have two management servers in ANY environment. A second management server allows for failover and easy restore. All management servers are members of the All Management Servers Resource pool, which balances the monitoring load of your management group as new management servers are added, and provides automatic failover for monitoring. See [Distributed Deployment of Operations Manager](#) for complete details.

Make sure the SDK Service is running on all management servers and that any SDK client (console, web console, connector, PowerShell) can connect to it. In System Center 2012 – Operations Manager, setup sets this service to automatically start on every management server during installation. We support any SDK client connecting to any management server.

Network Monitoring

See Considerations when Designing a Management Group for Network Monitoring for information regarding management packs and running Network Discovery.

Considerations for a Clean Installation of System Center 2012 – Operations Manager

The [Deployment Guide for System Center 2012 - Operations Manager](#) covers the full details of installing Operations Manager, in two installation scenarios:

1. [Single-Server Deployment of Operations Manager](#) - for evaluation, testing, and management pack development, usually in nonproduction or preproduction environments
2. [Distributed Deployment of Operations Manager](#) - forms the foundation of 99 percent of Operations Manager deployments. It allows for the distribution of features and services across multiple servers to allow for scalability. It can include all Operations Manager server roles and supports the monitoring of devices across trust boundaries through the use of the gateway server

For the purposes of design and planning this topic will focus on design considerations for a distributed deployment making use of multiple management servers and the use of resource pools.

If you have not reviewed **Getting Started** or **Operations Manager 2012 Supported Configurations**, you may want to before continuing. These documents contain key concepts and important configuration details.



Note

Unified Installer is a utility designed to perform new, clean installations of System Center 2012 for testing and evaluation purposes only. If you want to upgrade from an existing System Center installation or choose any set up options such as high availability or multi-server component installs, we recommend you refer instead to the procedures detailed in the deployment guides for each individual System Center 2012 component.

Common Installations

Use the [Operations Guide for Operations Manager for System Center 2012](#) to determine hardware requirements for each Operations Manager server feature. If you want to install more than one feature on the same computer, use the higher of the recommended hardware requirements for any of the combined features.

The sizing helper is a downloadable tool in spreadsheet format that contains tabs listing general information on supported configurations, as well as sizing examples based on number of agents and number of network devices monitored, information on gateway servers, and more.

For example, a scenario calling for 500 agents monitoring 50 network devices calls for a recommendation of:

1. (1) One management server managing up to 500 agents handling the entire workload, plus (1) one additional management server for HA / failover, managing up to five SDK connections
2. (2) Two management servers in a single resource pool monitoring the 50 network devices
3. (2) Two servers: An Operations Database Server, and an Operations Data Warehouse Server (with an SRS and Web Console Server)

Not included in this scenario is the possible need for a gateway server. They are supported for use in managing network devices, but the gateway server must be in its own resource pool, and not in the same pool as the devices.

Resource Pools

A resource pool is a collection of management servers or gateway servers used to distribute work amongst themselves and to take over work from a failed member.

Due to the introduction of resource pools it is recommended that all management servers be connected by a low latency network. This means that if you are currently using management servers in multiple datacenters or sites we recommend you move all management servers to a single data center and use gateway servers at the other sites.

You should always have two management servers in ANY environment. A second management server allows for failover and easy restore. All management servers are members of the All Management Servers Resource pool, which balances the monitoring load of your management group as new management servers are added, and provides automatic failover for monitoring. See [Distributed Deployment of Operations Manager](#) for complete details.

Make sure the SDK Service is running on all management servers and that any SDK client (console, web console, connector, PowerShell) can connect to it. In System Center 2012 – Operations Manager, setup sets this service to automatically start on every management server during installation. Any SDK client can connect to any management server.

Considerations when Designing a Management Group for Network Monitoring

System Center 2012 – Operations Manager provides the ability to discover and monitor network routers and switches, including the network interfaces and ports on those devices and the virtual

LAN (VLAN) that they participate in. You can also delete discovered network devices and prevent the deleted network devices from being rediscovered the next time discovery runs. For more information, see **Monitoring Networks by Using Operations Manager**.

Resource Pools

Network monitoring in System Center 2012 – Operations Manager requires its own separate resource pool.

Create a resource pool dedicated to network management; add dedicated management servers into the newly created resource pool, then remove the dedicated management server from any other resource pool.

1. Each management server or gateway server can run only one discovery rule. You specify a single management server or gateway server to run the discovery rule and a management server resource pool to perform the actual monitoring of the network devices.
2. If you create discovery rules on multiple management servers, you should create a management pool for each and make sure that each discovery defines a different set of devices. If a single device is managed in different pools, it will not be able to be deleted.

For more information see **How to Discover Network Devices in Operations Manager 2012** and **Network Device Discovery Settings**.

Performance and Scale

Because network monitoring workflows run on management servers (on the SNMP module), and not on agents, a heavy load is placed on the management servers. Therefore for better performance we recommend using dedicated management servers in dedicated resource pools for network monitoring.

For more information see the [Operations Manager Sizing Helper](#).

Network Device Accessibility

Network devices must be accessible by the management servers during monitoring.

1. Any firewalls between the management servers and the devices must be considered in planning, and when setting up dedicated resource pools.
2. Gateway servers are supported for use in managing network devices, but the gateway server must be in its own resource pool, and not in the same pool as the devices.

Upgrade

If you were monitoring network devices in Operations Manager 2007 R2 and are upgrading to System Center 2012 – Operations Manager, the network monitoring you were performing will still function properly. But if you want to take advantage of the additional monitoring capabilities available when upgrading, you will need to rerun network device discovery. However, you must also upgrade any appropriate management packs. See **Monitoring Networks by Using Operations Manager** for more information. If upgrading management packs is not an option,

then do not rerun discovery: continue to operate under the original management packs and the original network monitoring capabilities you had under Operations Manager 2007 R2.

See Also

Security for Servers Performing Network Discovery

Tuning Network Monitoring

Considerations for Application Performance Monitoring

In Operations Manager, you can monitor Internet Information Services (IIS)-hosted .NET applications from server- and client-side perspectives to get details about application performance and reliability that can help you pinpoint root causes of incidents. For more information, see **.NET Application Performance Monitoring Template** in the Authoring Guide and **Monitoring .NET Applications** in the Operations Guide.

Operations Database

The primary consideration for application performance monitoring on design and planning is its impact on the database. Since application performance monitoring in Operations Manager is Health Service based, scale and load put on the Operations Manager Database is an important factor to consider.

For example, when monitoring many applications that generate several events (state changes) each per second, it is easy to see how the Health Services can be overloaded if not considered in the design phase. For example, the average application generates 0.3 events per second. With IIS supporting hundreds of applications per host it can result in 30 or more events being raised per second through the Health Service.

For more information see [Operations Manager Sizing Helper](#) and **How to Configure Grooming Settings for the Operations Manager Database**.

Agents

Application performance monitoring is not agentless, so using resource pools is not a design option for optimizing performance or scale. The application monitoring agent is installed at the same time as the Operations Manager agent. You do not have to pre-plan where to install the application monitoring service.

Upgrade

For AVIcode 5.7 customers, there are two ways to look at an upgrade:

1. Integrated (AVIcode integrated with Operations Manager), where Operations Manager handles some of the configuration steps
2. Standalone (Continuing to run AVIcode 5.7 as a separate product from Operations Manager)

For more information, see **Notes for AVIcode 5.7 Customers** in the Operations Guide.

Note: Installation of AVIcode 5.7 integration management packs is NOT supported in System Center 2012 – Operations Manager. If you need to use AVIcode 5.7 with System Center 2012 – Operations Manager, for example to monitor IIS 6 hosts, the management packs must be installed on the System Center Operations Manager 2007 R2 environment before upgrading to System Center 2012 – Operations Manager. Additionally, you need to import an update for the AVIcode 5.7 management packs from the System Center 2012 – Operations Manager installation media.

See Also

Monitoring .NET Applications

Considerations for High Availability and Disaster Recovery

This section describes key concepts to consider when designing for disaster recovery. Using multiple management servers and the concept of resource pools, it is possible to easily set up for successful failover scenarios.

Multiple Management Servers and Distributed Deployment

You should always have two management servers in ANY environment. A second management server allows for failover and easy restore, and a second management server can take on the load if one fails. All management servers are members of the All Management Servers Resource pool, which balances the monitoring load of your management group as new management servers are added, and provides automatic failover for monitoring. The impact of failure of a management server in a distributed environment is minimized, but it increases the workload on additional management servers in the management group until the failed management server is restored. See [Distributed Deployment of Operations Manager](#) in the Deployment Guide for complete details.

You should always keep a backup of your operational database and data warehouse databases. For information about scheduling regular backups of the Operations Manager databases, see [How to Schedule Backups of System Center 2012 - Operations Manager Databases](#).

You must keep SDK services running on all management servers.

See Also

[Operations Manager Sizing Helper](#)

Deploying System Center 2012 - Operations Manager

All System Center 2012 – Operations Manager individual management group deployments will either be an "all-in-one" installation, where all features are loaded on a single server, or the deployment will be a distributed installation, where Operations Manager features are distributed

across servers. Any number of these can then be combined together to form an overall Operations Manager infrastructure that consists of multiple management groups. These management groups can then relate to each other in a hierarchical fashion as your business needs dictate.

This section of the Deployment Guide describes an individual management group deployment, where you have one management group, but the features of Operations Manager are either installed on a single server or distributed over several servers.

- [Single-Server Deployment of Operations Manager](#)
- [Distributed Deployment of Operations Manager](#)

For information about connecting management groups, see [Connecting Management Groups in Operations Manager](#).

Before You Begin

Before you begin your deployment, you should read the release notes, and ensure that your server meets the minimum system requirements for Operations Manager. For more information, see:

- [Release Notes for System Center 2012 - Operations Manager](#)
- [System Requirements for System Center 2012 – Operations Manager](#)

Operations Manager Administrators Role Assignment

Operations Manager handles assignment of the Operations Manager Administrators role differently than previous versions. In System Center 2012 – Operations Manager, Setup automatically assigns the Administrators group on the local computer to the Operations Manager Administrators role. You must be logged on with an account that has local Administrator rights to run Setup on the first management server that you install; this ensures that you can open the Operations console after Setup is completed. When you install additional management servers, you must use a Domain account of which you are a member.

Required Accounts

During setup, you are prompted for two accounts, the **management server action account** and the **System Center Configuration service and System Center Data Access service** account. In Operations Manager, you can use the same account for both services.

If you install Reporting, you are prompted for two additional accounts, the **Data Warehouse Write account** and the **Data Reader account**. These accounts are created as domain user accounts and added to the local Administrators group on the target server.





Note

If you create a specific account for installation, this account must be a member of the **sysadmin** server role for Microsoft SQL Server, but also have access to the master database.

**Note**

If you install multiple management servers, you are prompted for a **management server action account** and a **System Center Configuration service and System Center Data Access service account** each time you add a management server. You must provide the same accounts for each installation.

Account	Description	Permissions
Management server action account	This account is used to carry out actions on monitored computers across a network connection.	To save time, specify a domain-based account. We recommend that you create an account for this purpose that has local administrative credentials. You should not use an account that has domain administrative credentials.
System Center Configuration service and System Center Data Access service account	This account is one set of credentials that is used to update and read information in the operational database. Operations Manager ensures that the credentials used for the System Center Data Access service and System Center Configuration service account are assigned to the sdk_user role in the operational database.	This account can be configured as either Local System or as a domain account. The account must have local administrative credentials. For cases where the operational database is hosted on a remote computer that is not a management server, a domain account must be used. For better security, we recommend that you use an account different from the one used for the management server action account.
Data Warehouse Write account	The Data Warehouse Write account writes data from the management server to the Reporting data warehouse and reads data from the operational database.	<p>This account is assigned write permissions on the Data Warehouse database and read permissions on the operational database.</p> <p> Note Ensure that the account you plan to use for the Data Warehouse Write account has SQL Server Logon rights and has logon rights for the</p>

Account	Description	Permissions
		computers hosting both the operational database and the reporting data warehouse. Otherwise, Setup fails, and all changes are rolled back. This might leave SQL Server Reporting Services in an inoperable state.
Data Reader account	The Data Reader account is used to define which account credentials SQL Server Reporting Services uses to run queries against the Operations Manager reporting data warehouse.	The account should be configured as a domain account.  Note Ensure that the account you plan to use for the Data Reader account has SQL Server logon rights and Management Server logon rights.

SQL Server Requirements

System Center 2012 – Operations Manager requires access to an instance of a server running Microsoft SQL Server 2008 SP1, SQL Server 2008 R2, or SQL Server 2008 R2 SP1. This instance can be located on a separate computer from the management servers in a distributed installation or on the first management server in the management group. In either case, the instance of Microsoft SQL Server 2008 SP1, SQL Server 2008 R2, or SQL Server 2008 R2 SP1 must already exist and be accessible before you start your first management server installation. The SQL Server Collation setting must be a supported value, and SQL Full Text Search must be enabled.

System Center 2012 Service Pack 1 (SP1), Operations Manager requires access to an instance of a server running Microsoft SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1. This instance can be located on a separate computer from the management servers in a distributed installation or on the first management server in the management group. In either case, the instance of Microsoft SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1 must already exist and be accessible before you start your first management server installation. The SQL Server Collation setting must be a supported value, and SQL Full Text Search must be enabled.

During setup, you are prompted for the following:

- The SQL Server database server name and instance name. If you have installed SQL Server by using the default instance, you only have to specify the SQL Server name.

You can accept the default values for or set:

- SQL Server Port number. By default, 1433.
- A new operational database (for first management server installation in the management group) or an existing operational database (for installing additional management servers in an existing management group).
- The database name. By default, OperationsManager.
- The starting database size. By default, 1000 MB.
- The Data file and Log folder locations. By default, these are C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Data or C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log as appropriate to the SQL Server defaults.



Important

If TCP/IP is disabled on a remote server that is hosting the SQL Server database, Setup will not be able to connect to the SQL Server database. To resolve this issue, enable TCP/IP on the remote server.

Ensure that SQL Server Reporting Services has been correctly installed and configured. For more information about how to install and configure SQL Server 2012 Reporting Services, see [SQL Server Installation \(SQL Server 2008 R2\)](#).

See Also

[Deploying System Center 2012 - Operations Manager](#)

Environmental Prerequisites for Operations Manager

This section covers the infrastructure that you need to have in place and other factors to consider before you run the Setup for System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager.

There are two sets of prerequisites that must be satisfied prior to installing any of the Operations Manager features. One set consists of those items that the Prerequisite checker identifies during Setup. The Prerequisite checker is targeted at the server that Setup is running on and determines if the server has the necessary configuration to host whatever role you have chosen.

The other set consists of those items that are outside the scope of the Prerequisite checker, such as the Active Directory domain or forest functional level, or the availability of a certification authority (CA) to issue the certificates that are necessary for deploying agents and gateway servers across trust boundaries. This section addresses this second set of prerequisites, which are much broader in scope, because they apply to the whole environment that Operations Manager will be functioning in, rather than those that are verified by the Prerequisite checker during Setup. To ensure that Operations Manager deploys smoothly and functions as expected, the environment that it will run in must be properly prepared. Because environmental changes affect more than Operations Manager, ensure that you exercise due caution before making

sweeping changes. The prerequisites are presented in a unified format with scenario-specific items called out.

For more information about design and environmental decisions, see [Planning the System Center 2012 - Operations Manager Deployment](#). For more information about supported configurations for System Center 2012 – Operations Manager, see [System Requirements for System Center 2012 – Operations Manager](#).

In This Section

Supporting Infrastructure

Describes prerequisites and issues that you need to be aware of before you install System Center 2012 – Operations Manager.

Security Considerations

Describes high-level security factors that need to be addressed.

Agent and Agentless Monitoring

Describes the environmental prerequisites for deploying agents to monitor devices and for deploying agentless monitoring.

Supporting Infrastructure

This section addresses prerequisites and issues involving Active Directory Domain Services (AD DS) and Domain Name System (DNS) that you need to be aware of before initiating your System Center 2012 – Operations Manager installation.

Active Directory Domain Services

System Center 2012 – Operations Manager relies on AD DS for a number of services, including definition of security principles, rights assignment, authentication, and authorization. Operations Manager queries AD DS when performing computer and service discovery and can use AD DS for storing and distributing agent configuration information. For Operations Manager to function properly, AD DS and its supporting service, DNS, need to be healthy and at certain minimum configuration levels. In addition, certain domain naming conventions must be followed.

Domain Space Naming

An Operations Manager management group cannot be installed into a root Active Directory domain that has a flat DNS namespace. However, you can install the management group into child domains of the root domain. For example, you have a root domain that has a DNS name of "Woodgrove". Because this root domain has a flat DNS namespace, you cannot install an Operations Manager management group into the Woodgrove domain. But, if the Woodgrove

domain has a child domain with a DNS name of "National", the fully qualified domain name of the child domain would be national.woodgrove. For more information about configuring Windows for domains with single-label DNS names, see [Information about configuring Active Directory domains by using single-label DNS names](#).

Domain Functional Level

Windows Server Active Directory can operate at different functional levels. These levels are distinguished by the version of the Windows Server operating system that is permitted on the domain controllers present in the domain. System Center 2012 – Operations Manager requires that the domain functional level be Windows 2000 native, Windows Server 2003 interim, Windows Server 2003, or Windows Server 2008. The domain functional level of Windows Server 2008 R2 is also supported (for the SP1 version of System Center 2012 – Operations Manager, Windows Server 2008 R2 SP1 and Windows Server 2012 are supported). For System Center 2012 – Operations Manager to function properly, you must check the domain functional level and raise it to the appropriate version. To do this, see [Raise the Domain Functional Level](#).



Note

Ensure that you exercise due caution prior to raising a domain's functional level because it cannot be reversed, and if there are any down-level domain controllers, their function will be impacted.

Forest Functional Level

The forest functional level is similar to the domain functional level in that it sets a minimum domain controller operating system level across the whole forest. After it is set, domain controllers with down-level operating systems from lower functional levels cannot be introduced into the forest. Operations Manager does not have a forest functional level requirement; however, if the forest functional level is left at the default Windows 2000 level, there may be domains in your forest that won't meet the minimum domain functional level requirement.

DNS

DNS must be installed and in a healthy state to support AD DS. Beyond the reliance of Operations Manager on AD DS, there are no specific DNS requirements.

See Also

[Environmental Prerequisites for Operations Manager](#)

Security Considerations

Most of the work in preparing the environment for System Center 2012 – Operations Manager goes into security-related tasks. This section covers those tasks at a cursory level. For more information, see the [Index to Security-related Information for Operations Manager](#).

Preparing the security-related tasks involves the following:

- Understanding, planning, and preparing for monitoring across trust boundaries.
- Understanding, planning, and preparing for monitoring UNIX or Linux computers.

- Planning and preparing the service accounts, user accounts, and security groups that you will need.
- Understanding and preparing the network ports as required by your design.

Trust Boundaries

Active Directory domains form the basic unit of a Kerberos trust boundary as seen by Operations Manager. This boundary is automatically expanded to other domains in the same name space (the same Active Directory tree), and between domains that are in different Active Directory trees but still in the same Active Directory forest via transitive trusts. The trust boundary can be further expanded between domains in different Active Directory forests through the use of across forest trusts.

Kerberos

The Kerberos authentication protocol, which is supported by Windows 2000 domain controllers and above, can only occur within a trust boundary. Kerberos authentication is the mechanism used to perform the Operations Manager agent/server mutual authentication. Agent/server mutual authentication is mandated in Operations Manager Shell for all agent/server communication.

An Operations Manager management group does have the ability to perform discovery and monitoring outside of the Kerberos trust boundary that it is in. However, because the default authentication protocol for Windows-based computers that are not joined to an Active Directory domain is NTLM, another mechanism must be used to support mutual authentication. This is done through the exchange of certificates between agents and servers.

Certificates

When Operations Manager communication needs to occur across trust boundaries, such as when a server that you want to monitor lies in a different, untrusted, Active Directory domain than the management group that is performing the monitoring, certificates can be used to satisfy the mutual authentication requirement. Through manual configuration, certificates can be obtained and associated with the computers and the Operations Manager services running on them. When a service that needs to communicate with a service on a different computer starts and attempts to authenticate, the certificates will be exchanged and mutual authentication completed.

Important

The certificates used for this purpose must ultimately trust the same root certification authority (CA).

For more information about how to obtain and make use of certificates for mutual authentication, see [Deploying a Gateway Server](#).

Certification Authority

To get the necessary certificates, you will need access to a certification authority (CA). This can be either Microsoft Certificate Services or a third-party certification service such as VeriSign.

Microsoft Certificate Services

There are four types of Microsoft CAs:

- Enterprise root

- Enterprise subordinate
- Stand-alone root
- Stand-alone subordinate
- Both enterprise types of CAs require Active Directory Domain Services; stand-alone CAs do not. Either type of CA can issue the necessary certificates for agent/server mutual authentication across trust boundaries.

Customarily, a CA infrastructure consists of a root CA that signs its own certificates and certifies itself and one or more subordinate CAs, which are certified by the root. The subordinate CA servers are the ones that a service certificate requests, while the root is taken offline and held for safekeeping. For more information about designing certificates, see [Infrastructure Planning and Design](#) and [Authentication and Data Encryption for Windows Computers](#).

Monitoring UNIX and Linux computers

System Center 2012 – Operations Manager can monitor UNIX and Linux computers. Because the UNIX and Linux computers are not participating in the Active Directory domain that the management group is in a variation of the certificate method of mutual authentication, discussed before, is used.

Establishing Mutual Authentication with UNIX and Linux computers

You will use the Discovery wizard to find UNIX and Linux computers and add them to the management group as managed objects. During the Discovery wizard process, Operations Manager has the discovered UNIX and Linux computer generate a self-signed certificate which is used for mutual authentication with the management server. The certificate generation, signing and exchange process works like this when SSH discovery is enabled:

1. The Discovery Wizard process on the management server has the discovered UNIX or Linux computer generate a self-signed certificate.
2. The discovering management server issues a get certificate request to the UNIX or Linux computer.
3. The UNIX or Linux computer returns the certificate to the management server
4. The discovering management server creates a key pair and a self-signed certificate of its own. The management server only generates a key pair and a self-signed certificate when it discovers its first UNIX or Linux computer. The management server then imports its own certificate into its trusted certificate store. The discovering management server then signs the UNIX or Linux certificate with its private key. Any subsequent signing of UNIX or Linux computer certificates by the management server will reuse the management server's private key that was generated on the first signing.
5. The discovering management server then issues a put certificate request which puts the now management server-signed certificate back onto the UNIX or Linux computer that initially generated it. The UNIX or Linux computer WSMAN communication layer is then restarted to make the new UNIX/Linux computer generated certificate active.
6. Now when the management server requests that the UNIX or Linux computer authenticate itself, the UNIX or Linux computer will provide the trusted certificate to the management server and the management server will read the signature on the certificate that it is presented with, see that it trusts this signature (because the signature is its own private key

that is stored in its own trusted certificate store) and accept this certificate as proof that the UNIX OR LINUX computer is who the management server thinks it is.

7. The discovering management server will use UNIX or Linux credentials as configured in the appropriate Run As Profile to authenticate itself with the UNIX or Linux computer. See the [Planning for UNIX or Linux Run As Profiles](#) section for more details.

Important

The preceding order of operations is for the low security version of UNIX or Linux discovery.

Planning for UNIX or Linux Run As Profiles

After the UNIX or Linux computer is being managed by the discovering management server, the management pack discoveries and workflows begin to run. These workflows require the use of credentials to complete successfully. These credentials, what objects, classes or group they will be applied to and the computers that they will be distributed to are contained in Run As Profiles. There are two Run As Profiles that are imported when the UNIX management packs are imported into your management group; they are:

- Unix Action Account profile – This Run As profile and its associated UNIX or Linux credentials are used for low security activities on the designated UNIX or Linux computers.
- Unix Privileged Account profile – This Run As profile and its associated UNIX or Linux credentials are used for activities that are protected by a higher level of security and therefore require an account that has higher privileges on the UNIX or Linux computer. This can be (but does not have to be) the root account.

You will need to configure these profiles with the appropriate UNIX or Linux computer credentials for the management pack workflows that use them to function correctly.

Accounts and Groups

Over the lifetime of your Operations Manager deployment, you will potentially need many accounts and security groups. During Operations Manager Setup, you are only prompted for four. You need to consider additional accounts when planning out role-based security assignments, notifications, and alternate credentials to run processes. For guidance on planning role-based security assignments, see [Planning the System Center 2012 - Operations Manager Deployment](#).

Role-Based Security Accounts and Groups

Operations Manager controls access to monitored groups, tasks, views, and administrative functions through the assignment of user accounts to roles. A role in Operations Manager is the combination of a profile type (operator, advanced operator, administrator) and a scope (what data the role has access to). Typically, Active Directory security groups are assigned to roles, and then individual accounts are assigned to those groups. Prior to deploying, plan out Active Directory security groups that can be added to these and any custom-created roles so that you can then add individual user accounts to the security groups.

Operations Manager provides the following role definitions out-of-the-box.

Role name	Profile type	Profile description	Role scope
Operations Manager Administrators: Created at setup; cannot be deleted; must contain one or more global groups	Administrator	Has full privileges to Operations Manager; no scoping of the Administrator profile is supported	Full access to all Operations Manager data, services, administrative, and authoring tools
Operations Manager Advanced Operators: Created at setup; globally scoped; cannot be deleted	Advanced Operator	Has limited change access to Operations Manager configuration; ability to create overrides to rules; monitors for targets or groups of targets within the configured scope	Access to all groups, views, and tasks currently present and those imported in the future
Operations Manager Authors: Created at setup; globally scoped; cannot be deleted	Author	Has ability to create, edit, and delete tasks, rules, monitors, and views within configured scope	Access to all groups, views, and tasks currently present and those imported in the future
Operations Manager Operators: Created at setup; globally scoped; cannot be deleted	Operator	Has ability to interact with alerts, run tasks, and access views according to configured scope	Access to all groups, views, and tasks currently present and those imported in the future
Operations Manager Read-Only Operators: Created at setup; globally scoped; cannot be deleted	Read-Only Operator	Has ability to view alerts and access views according to configured scope	Access to all groups and views currently present and those imported in the future
Operations Manager Report Operators: Created at setup; globally scoped	Report Operator	Has ability to view reports according to configured scope	Globally scoped
Operations Manager Report Security Administrators: Integrates SQL Server	Report Security Administrator	Enables integration of SQL Server Reporting Services security with Operations Manager	No scope

Role name	Profile type	Profile description	Role scope
Reporting Services security with Operations Manager user roles; gives Operations Manager administrators the ability to control access to reports; cannot be scoped		roles	

You can add Active Directory security groups or individual accounts to any of these predefined roles. If you do, those individuals will be able to exercise the given role privileges across the scoped objects.



Note

The predefined roles are globally scoped, giving them access to all groups, views, and tasks (except for Report Security Administrator).

Operations Manager also allows you to create custom roles based on the Operator, Read-Only Operator, Author, and Advanced Operator profiles. When you create the role, you can further narrow the scope of groups, tasks, and views that the role can access. For example, you can create a role entitled "Exchange Operator" and narrow the scope to only Exchange-related groups, views, and tasks. User accounts assigned to this role will only be able to run Operator-level actions on Exchange-related objects.

Notification Accounts and Groups

Individuals in your company that will interact with Operations Manager frequently, such as an Exchange administrator who has been assigned to the Exchange Operator role, need a way to discover new alerts. This can be done by either watching the Operations console for new alerts or by Operations Manager informing them about the alert via supported communications channels. Operations Manager supports notifications through e-mail, instant messaging, Short Message Service, or pager messages. Notifications on what the role needs to know go out to recipients that you specify in Operations Manager. An Operations Manager recipient is merely an object that has a valid address to receive the notification, such as an SMTP address for e-mail notifications.

Therefore, it is logical to combine role assignment with notification group membership via an e-mail-enabled security group. For example, create an Exchange Administrators security group and populate it with individuals that have the knowledge and permissions to fix things in Exchange. Assign this security group to a custom-created Exchange Administrator role so they have access to the data and are e-mail-enabled. Then, create a recipient by using the SMTP address of the e-mail-enabled security group.

Service Accounts

At the time of deployment, you need to have the following service accounts ready. If you use domain accounts and your domain Group Policy object (GPO) has the default password expiration policy set as required, you will either have to change the passwords on the service accounts according to the schedule, or use low maintenance system accounts, or configure the accounts so that the passwords never expire.

Account name	Requested when	Used for	Low maintenance	High security
Management server Action Account	management server setup	Collecting data from providers, running responses	Local system	Low privilege domain account
Data Access Service and Configuration Service Account	management server setup	Writing to operational database, running services	Local system	Low privilege domain account
Local Administrator Account for target devices	Discovery and push agent install	Installing agents	Domain or local administrator account	Domain or local administrator account
Agent Action Account	Discovery and push agent install	Gathering information and running responses on managed computers	Local system	Low privilege domain account
Data Warehouse Write Action Account	Reporting Server setup	Writing to the Reporting Data Warehouse database	Low privilege domain account	Low privilege domain account
Data Reader Account	Reporting Server setup	Querying SQL Reporting Services database	Low privilege domain account	Low privilege domain account

Service Principal Names

When you deploy Operations Manager, you may need to register a Service Principal Name (SPN) in some configurations. SPNs are used by Kerberos authentication for the client to mutually authenticate with the server. For more information, see [What Are Service Publication and Service Principal Names?](#).

When you install Operations Manager, you select an account for the **System Center Configuration service and System Center Data Access service**. For more information, see [Deploying System Center 2012 - Operations Manager](#).

 **Caution**

Do not modify the default Active Directory permissions to allow an account to do unrestricted modifications of its own SPN.

If you select the Local System as the System Center Data Access service account, the account can create the appropriate SPN. No additional configuration is necessary.

If you use a domain account, you must register an SPN for each management server. Use the SETSPN command line tool. For more information about running that tool, see [Setspn Overview](#).

Register both the netbios name and fully qualified domain name of the management server, using the following syntax:

```
setspn -a MSOMSdkSvc/<netbios name> <DAS account domain>\<DAS account name>
```

```
setspn -a MSOMSdkSvc/<fqdn> <DAS account domain>\<DAS account name>
```

 **Tip**

You can list the SPNs registered to user account or computer with the following syntax:

```
setspn -l <DAS account name>
```

```
setspn -l <fqdn>
```

If you are using Network Load Balancing or using a hardware load balancer, the System Center Data Access service must run under a domain account. In addition to the setup already described, you must also register the load balanced name, using the following syntax:

```
setspn -a MSOMSdkSvc/<load balanced name> <DAS account domain>\<DAS account name>
```

 **Note**

All of the System Center Data Access services running behind the load balancer must be running with the same domain account.

Run As Accounts

Agents on monitored computers can run tasks, modules, and monitors on demand as well as in response to predefined conditions. By default, all tasks run by using the Agent Action account credentials. In some cases, the Agent Action account may have insufficient rights and privileges to run a given action on the computer. Operations Manager supports the running of tasks by agents in the context of an alternate set of credentials called a Run As Account. A Run As Account is an object that is created in Operations Manager, just like a recipient is, and maps to an Active Directory user account. A Run As Profile is then used that maps the Run As Account to a specific computer. When a rule, task, or monitor that has been associated with a Run As Profile at the development time of a management pack needs to run on the targeted computer, it does so by using the specified Run As Account.

Out-of-the-box, Operations Manager provides a number of Run As Accounts and Run As Profiles, and you can create additional ones as necessary. You may also choose to modify the Active Directory credentials that a Run As Account is associated with. This will require planning,

creating, and maintaining additional Active Directory credentials for this purpose. You should treat these accounts as service accounts with respect to password expiration, Active Directory Domain Services, location, and security.

You will need to work with management pack authors as they develop requests for Run As Accounts. For more information, see the [Index to Security-related Information for Operations Manager](#).

See Also

[Environmental Prerequisites for Operations Manager](#)

Agent and Agentless Monitoring

This section covers the environmental prerequisites for devices that will have agents installed and devices that will be monitored in an agentless fashion.

Clients with Agents Installed

The three main activities involved with agent administration are discovery of target devices, deployment or installation of agents to those devices, and ongoing management of the agents. Agents that lie outside a trust boundary require a few more prerequisites than agents that lie inside a trust boundary.

Agents Inside a Trust Boundary

Discovery

Discovery requires that the TCP 135 (RPC), RPC range, and TCP 445 (SMB) ports remain open and that the SMB service is enabled. For UNIX/Linux computers, default discovery and management occurs over TCP 1270, troubleshooting, and diagnostics discovery occur over SSH, TCP 22. Discovery and deployment over SSH, default TCP 22, can also be enabled to allow Operations Manager to install the WSMAN communication layer on the discovered UNIX/Linux computer.

Installation

After a target device has been discovered, an agent can be deployed to it. Agent installation requires the following:

- Opening Remote procedure call (RPC) ports beginning with endpoint mapper TCP 135 and the Server Message Block (SMB) port TCP/UDP 445.
- Enabling the File and Printer Sharing for Microsoft Networks and the Client for Microsoft Networks services (this ensures that the SMB port is active).
- If enabled, Windows Firewall Group Policy settings for **Allow remote administration exception** and **Allow file and printer sharing exception** must be set to **Allow unsolicited incoming messages from:** to the IP address and subnets for the primary and secondary management servers for the agent.
- An account that has local administrator rights on the target computer.
- Windows Installer 3.1. To install, see [Windows Installer 3.1](#) (article 893803) in the Microsoft Knowledge Base.

- Microsoft Core XML services (MSXML) 6 on the Operations Manager product installation media in the \msxml subdirectory.

**Note**

Push agent installation will install MSXML 6 on the targeted device if it is not there.

Ongoing Management

Ongoing management of an agent requires that the TCP 135 (RPC), RPC range, and TCP 445 (SMB) ports remain open and that the SMB service remains enabled.

Agents Outside a Trust Boundary

For agents that lie outside the trust boundary of the management servers, the environmental prerequisites are the same as for those that lie inside a trust boundary, plus some additions.

Because the device is going to have an installed agent, the software, service, and port requirements remain the same. However, because there is no underlying infrastructure to support Kerberos authentication, certificates must be used on both sides of the connection.

To simplify the cross trust boundary configuration, you can install an Operations Manager gateway server in the same trust boundary as the devices that you will monitor. The gateway server acts as a proxy so that all communication between the management server and agents is routed through the gateway server. This communication is done over a single port, TCP 5723, and requires certificates on the management server and the gateway server. In addition, the gateway server performs discovery and installation, and relays ongoing administration traffic on behalf of the management server to the agents. The use of gateway servers also reduces the volume of network traffic and is therefore useful in low bandwidth conditions.

Gateway servers can also discover and manage UNIX/Linux computers; this is done over TCP ports 1270 and as needed SSH TCP 22, this port is configurable.

For more information about gateway server configuration, see [Deploying a Gateway Server](#).

Manually Installed Agents

Discovery is not performed for manually installed agents, so there are fewer requirements.

Agentless Monitoring

Agentless monitoring of devices is performed by either a management server or by another device that does have an agent, called a proxy agent. An agentless managed device must not be separated from its management server or proxy agent by a firewall because monitoring is performed over RPC. The action account of the agent that is performing the monitoring must have local administrative rights on the device that is being monitored.

See Also

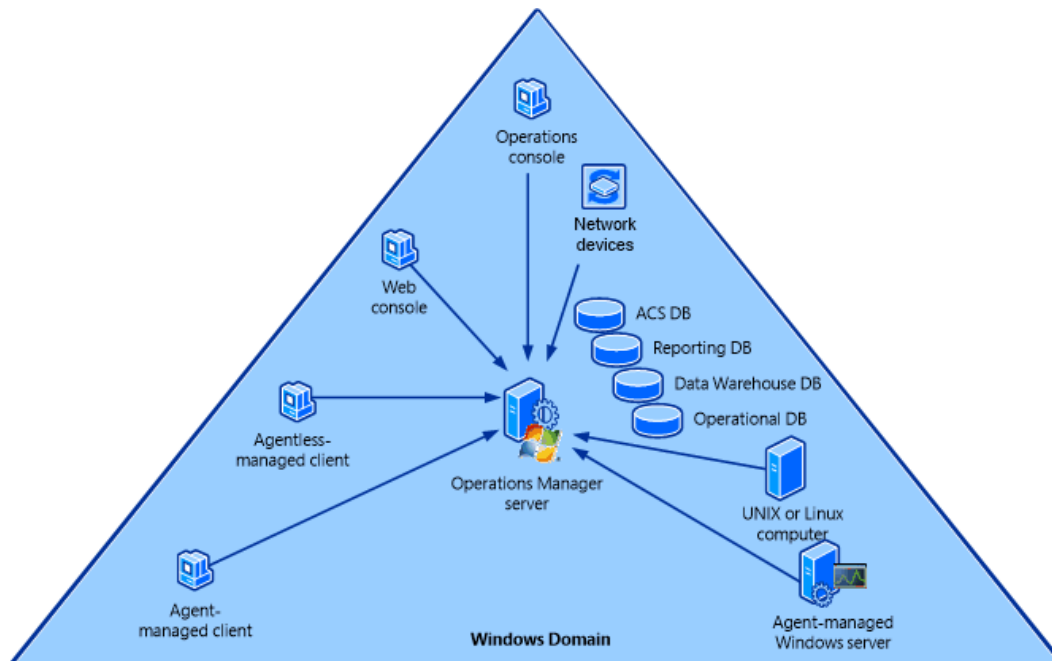
[Environmental Prerequisites for Operations Manager](#)

Single-Server Deployment of Operations Manager

The single-server management group scenario combines all the management group roles that can coexist onto a single instance of the Windows Server 2008 R2 SP1, or Windows Server 2012

operating system running as a member server in an Active Directory domain. This instance can be on dedicated hardware or on a virtual computer. The Operations console can be deployed to computers other than the single server, and the web console is accessed via a browser. Agents are then typically deployed to a limited number of devices depending on the capacity of the server that System Center 2012 – Operations Manager is deployed on.

You deploy Operations Manager in a single-server management group when you want to use it for evaluation, testing, and management pack development, usually in nonproduction or preproduction environments.



Operations Manager Services

The single-server management group configuration supports the following services:

1. Monitoring and alerting
2. Reporting (available in the Operations console but not in the web console)
3. Audit collection
4. Agentless exception management
5. Data (accessed by using the web console and the Operations console)

Operations Manager Features

The single-server management group configuration combines these features:

- Audit Collection Services (ACS) collector
- ACS database
- ACS forwarder

- Operational database
- Operations console
- Reporting data warehouse database
- Reporting database
- Reporting server
- Web console server
- Command Shell

Restrictions

The single-server management group configuration is the easiest to deploy, but there are limitations to its capabilities and therefore limitations to what it is commonly used for.

Gateway Server

This configuration does not include the gateway server role. Because of this, all monitored devices must be in the same Active Directory forest as the management server or you must use certificates on both the managed computer and the management server to provide for mutual authentication.

High Availability and Redundancy

The single server, single management group resides on a single set of hardware. This configuration supports only one instance of each server role and therefore cannot support agent failover between management servers.

Common Uses

This configuration is most commonly used for evaluation, testing, and management pack development purposes, usually in nonproduction or preproduction environments. Single-server management group configurations generally lack the robustness and performance to support anything but the smallest production loads.

Ports Used

In this configuration, you need to make sure that network ports are opened for communication between the agents and the management server, between the Operations console and the management server, and between the web console and the management server. All other inter-service communication occurs on the management server itself. The ports are as follows:

- Operations console to management server: TCP 5724
- Operations console to Reporting server: TCP 80
- Web console to web console server: selected web site port
- Agent to management server: TCP 5723
- ACS forwarder to ACS collector: TCP 51909
- Agentless management: occurs over remote procedure call

- Management server to UNIX/Linux computer: TCP 1270
- Management server to UNIX/Linux computer for special discovery and troubleshooting: TCP 22

For a complete listing of ports used, the direction of the communication, and if the ports can be configured, see [Supported Configurations for System Center 2012 – Operations Manager](#).

To deploy Operations Manager in a single-server management group, see [Walkthrough: Installing Operations Manager on a Single Server](#).

See Also

[Deploying System Center 2012 - Operations Manager](#)

[Distributed Deployment of Operations Manager](#)

Walkthrough: Installing Operations Manager on a Single Server

This walkthrough guides you through an installation of System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager on a single server. The features installed include the following:

- Management server
- Operations console
- Web console
- Reporting server

Prerequisites

You must ensure that your server meets the minimum supported configurations for Operations Manager. For more information, see [System Requirements for System Center 2012 – Operations Manager](#).

Important

Before you follow these procedures, read the [Before You Begin](#) section of [Deploying System Center 2012 - Operations Manager](#).

To install the single server management group configuration

1. Log on to the server by using an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started, Select features to install** page select the **Management server**, **Operations console**, **Web console**, and **Reporting server** features. To read more about each feature and its requirements, click **Expand all**, or expand the buttons next to each feature. Then click **Next**.
4. On the **Getting Started, Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager** or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and resolve any warnings or errors, and then click

Verify Prerequisites Again to recheck the system.



Note

Installation of the web console requires that ISAPI and CGI Restrictions in IIS be enabled for ASP.NET 4. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET v4.0.30319**, and then click **Allow**.



Important

You must install IIS before installing .NET Framework 4. If you installed IIS after installing .NET Framework 4, you must register ASP.NET 4.0 with IIS. Open a Command prompt window by using the **Run As Administrator** option and then run the following command:

```
%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r
```

6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration, Specify an installation option** page, select **Create the first Management server in a new management group**, type in a name for your management group and then click **Next**.



Note

After the management group name is set, it cannot be changed. The Management Group name cannot contain the following characters: , () ^ ~ : ; . ! ? " , ' ` @ # % \ / * + = \$ | & [] < > { }, and it cannot have a leading or trailing space. It is recommended that the Management Group name be unique within your organization if you plan to connect several management groups together.

8. On the **Configuration, Please read the license terms** page, review the Microsoft Software License Terms, select **I have read, understood, and agree with the license terms**, and then click **Next**.
9. When the **Configuration, Configure the operational database** page opens, in the **Server name and instance name** box, type the name of the server and the name of the SQL Server instance for the database server that will host the operational database. If you installed SQL Server by using the default instance, you only have to enter the server name. If you changed the default SQL Server port, you must type in the new port number in the **SQL Server port** box.

If you type an invalid SQL Server and instance name, you see a red circle with a white **X** in it appear to the left of the **Server name and instance name** and **SQL Server port** boxes.

The white **X** appears under the following circumstances:

- You entered an instance of SQL Server or a SQL Server port value that is not valid or that does not exist.
- The instance of SQL Server that you specified does not have the required configuration or features.

- You entered a value that is out-of-range (for example, port 999999).
- You entered an illegal character for that box (for example, server\instance%)

You can hover the cursor over the **Server name and instance** text box to view additional information about the error.

10. After you type the correct value for the SQL Server database server name, click the **SQL Server port** box so that Setup will attempt to validate the values you typed for the SQL Server name and for the port number.
11. In the **Database name**, **Database size (MB)**, **Data file folder**, and **Log file folder** box, we recommend that you accept the default values. Click **Next**



Note

These paths do not change if you connect to a different instance of SQL Server.



Important

You might receive a message about having the wrong version of SQL Server, or you might encounter a problem with the SQL Server Windows Management Instrumentation (WMI) provider. To resolve this problem, open a Command Prompt window, select **Run as administrator**, and then run the following command. In the command, replace the *<path>* placeholder with the location of SQL Server:

```
mofcomp.exe "<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof"
```



Note

The SQL Server model database size must not be greater than 100 MB. If it is, you might encounter an error in Setup regarding the inability to create a database on SQL due to user permissions. To resolve the issue, you must reduce the size of the model database.

12. When the **Configuration, Configure the data warehouse database** page opens, in the **Server name and instance name** box, type the server name and the name of the instance of SQL Server for the database server that will host the data warehouse database.
13. Because this is a single-server installation, accept the default value of **Create a new data warehouse database**.
14. In the **Database name**, **Database size (MB)**, **Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.



Important

You might receive a message about having the wrong version of SQL Server, or you might encounter a problem with the SQL Server Windows Management Instrumentation (WMI) provider. To resolve this problem, open a Command Prompt window, select **Run as administrator**, and then run the following command. In the command, replace the *<path>* placeholder with the location of SQL Server:

mofcomp.exe “<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof”.



Note

These paths do not change if you connect to a different instance of SQL Server.

15. On the **Configuration, SQL Server instance for reporting services** page, select the SQL Server database instance from the drop-down list. This drop-down list contains the SQL Server database instance name that was created when you installed SQL Server 2008 R2, SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1 and should be the name of the server on which you are installing Operations Manager. Click **Next**.
16. On the **Configuration, Specify a web site for use with the Web console** page, select **Default Web Site** or the name of an existing website. Select the option **Enable SSL** only if the website has been configured to use SSL, and then click **Next**.
17. On the **Configuration, Select an authentication mode for use with the Web console** page, select your option, and then click **Next**.
18. On the **Configuration, Configure Operations Manager accounts** page, we recommend that you use **Domain Account** option for the **Management Server Action Account, System Center Configuration service and System Center Data Access service, the Data Reader account, and the Data Writer account**.
Enter the credentials for a domain account in each field. The error icon will disappear after account validation. Click **Next**.
19. On the **Configuration, Help improve System Center 2012 - Operations Manager** page, select your options and click **Next**.
20. If Windows Update is not activated on the computer, the **Configuration, Microsoft Update** page appears. Select your options, and then click **Next**.
21. Review the options on the **Configuration, Installation Summary** page, and click **Install**. Setup continues.
22. When Setup is finished, the **Setup is complete** page appears. Click **Close** and the Operations console will open.

▶ To install the System Center 2012 - Operations Manager single server management group configuration by using the Command Prompt window

1. Log on to the server by using an account that has local administrative credentials.
2. Open the Command Prompt window by using the **Run as Administrator** option.



Note

Setup.exe requires administrator privileges because the Setup process requires access to system processes that can only be used by a local administrator.

3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.



Important

Use the `/WebConsoleUseSSL` parameter only if your website has Secure Sockets Layer (SSL) activated.

For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.



Important

The following command assumes that you specified the Local System for the Management server action account (`/UseLocalSystemActionAccount`) and Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.

```
/ActionAccountUser: <domain\username> /ActionAccountPassword: <password>
/DASAccountUser: <domain\username> /DASAccountPassword: <password>
setup.exe /silent /install
/components:OMServer,OMConsole,OMWebConsole,OMReporting
/ManagementGroupName: "<ManagementGroupName>"
/SqlServerInstance: <server\instance>
/DatabaseName: <OperationalDatabaseName>
/DWSqlServerInstance: <server\instance>
/DWDatabaseName: <DWDatabaseName>
/UseLocalSystemActionAccount /UseLocalSystemDASAccount
/DatareaderUser: <domain\username>
/DatareaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
/AcceptEndUserLicenseAgreement: [0|1]
/WebSiteName: "<WebSiteName>" [/WebConsoleUseSSL]
/WebConsoleAuthorizationMode: [Mixed|Network]
/SRSInstance: <server\instance>
/SendODRReports: [0|1]
/EnableErrorReporting: [Never|Queued|Always]
/SendCEIPReports: [0|1]
/UseMicrosoftUpdate: [0|1]
```

Verifying the Installation

▶ To confirm the health of the management server

1. In the Operations console, select the **Administration** workspace.

2. In **Device Management** select **Management Servers**. In the results pane, you should see the management server that you just installed with a green check mark in the **Health State** column.

▶ **To confirm the health of operations manager reports**

1. In the Operations console, in the navigation pane, click the **Reporting** button.



Note

After initial deployment, it can take up to 30 minutes for reports to appear.

2. Click **Microsoft ODR Report Library**, and then double-click any of the reports listed. The selected report is generated and displays in a new window.

By default, you should see the following reports:

- **Alerts Per Day**
- **Instance Space**
- **Management Group**
- **Management Packs**
- **Most Common Alerts**



Note

Selecting the management packs report is particularly useful at this point because it provides you with a full inventory of the management packs that have been installed on your server.

3. Close the report window.

Next Steps

Now that you have installed Operations Manager, you can deploy agents and start monitoring your applications, servers, and network devices. For more information, see [Managing Discovery and Agents](#) and [Operations Manager 2012 Monitoring Scenarios](#).

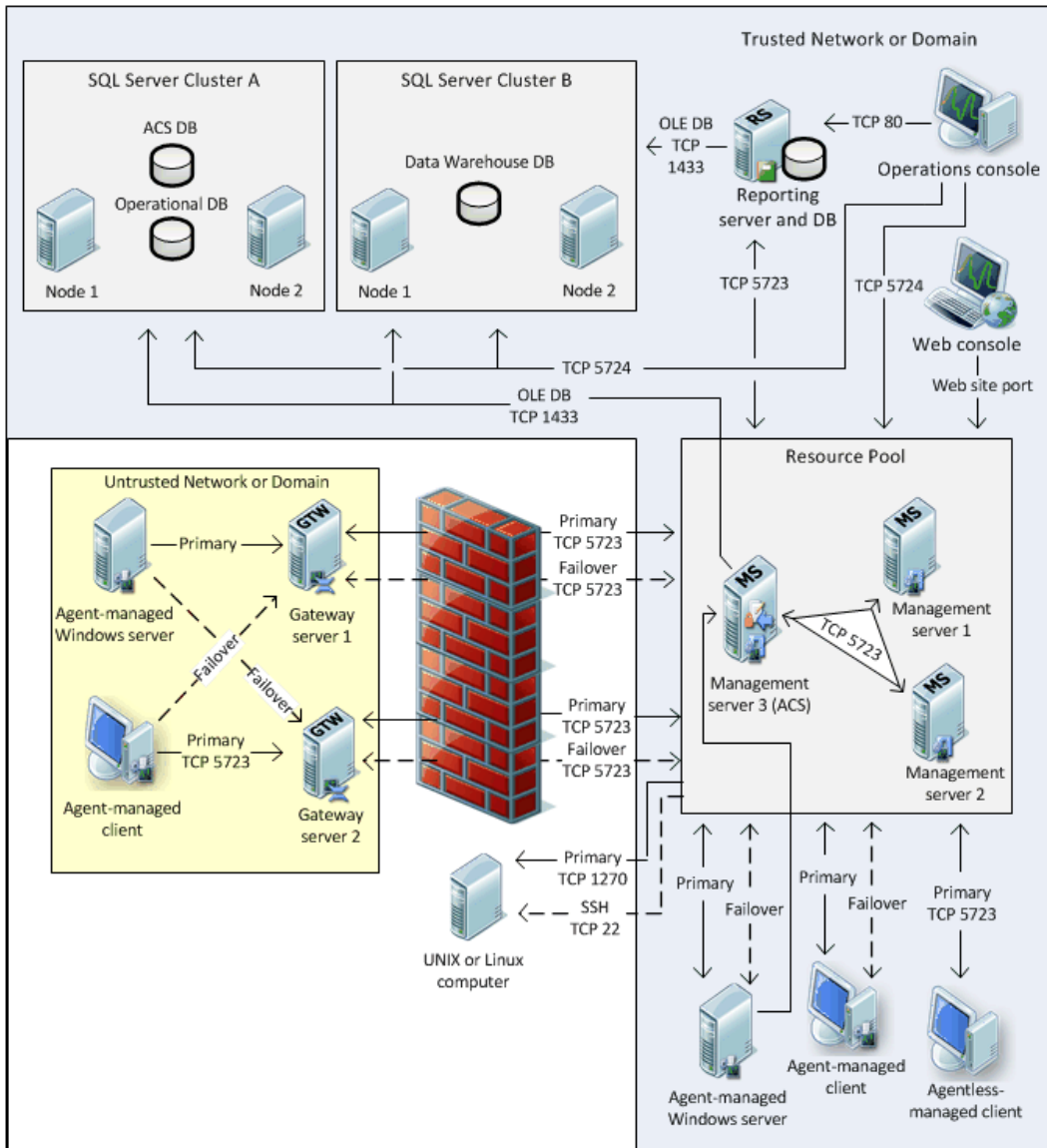
See Also

[Distributed Deployment of Operations Manager](#)

Distributed Deployment of Operations Manager

The distributed management group installation will form the foundation of 99 percent of Operations Manager deployments. It allows for the distribution of features and services across multiple servers to allow for scalability. It can include all Operations Manager server roles and supports the monitoring of devices across trust boundaries through the use of the gateway server.

The following diagram presents one possible option for the distributed management group topology.



Note

There is no direct communication between an operations console and the databases. All communication goes to the resource pool through TCP 5724, and then to the database servers using OLE DB on TCP 1433 or another customized port a customer establishes. However, there is direct communication between an Application Diagnostics console (residing with a web console) and databases.

System Center 2012 - Operations Manager Features

This configuration supports all System Center 2012 – Operations Manager and System Center 2012 Service Pack 1 (SP1), Operations Manager features:

- Monitoring and alerting, targeted for up to 15,000 agents
- Monitoring across trust boundaries
- Reporting
- Audit collection
- Agentless exception management
- Agent failover between management servers
- Gateway failover between management servers
- Clustering high availability for database roles

Operations Manager Servers

This configuration supports all Operations Manager server roles:

- Audit Collection Services (ACS) collector
- ACS database
- ACS forwarder (on agent-managed devices)
- Gateway server
- Management server
- Operational database
- Operations console
- For System Center 2012 – Operations Manager: SQL Server 2008 R2, or SQL Server 2008 R2 SP1 Reporting database
- For System Center 2012 Service Pack 1 (SP1), Operations Manager: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, SQL Server 2012 SP1 Reporting database
- Reporting data warehouse database
- Web console server

Restrictions

Single management group configurations do not support partitioning. Partitioning is the separation of management group services across multiple management groups. In Operations Manager, you may want to create multiple management groups for the following reasons.

Installed Languages

Operations Manager management groups support only one installed language. If the overall IT environment that you need to monitor has more than one installed language, a separate management group will be needed per language.

Consolidated Views

Even the largest distributed management group implementation will not be appropriate in every instance. This will lead you to implement multiple management groups, which will split your monitoring and alerting data between management groups. To provide a single, consolidated

view of your environment, data from multiple management groups can be consolidated and viewed in another management group. For more information, see [Connecting Management Groups in Operations Manager](#).

Function

You may need to have separate groups as needed according to function, such as preproduction for testing management packs and new servers, and production for monitoring daily business processes.

Administrative or Other Business Needs

Your company may have other administrative, security, or business needs that require complete separation of monitoring data and administrative teams, which will mandate additional management groups.

Common Uses

Distributed management groups are most commonly used to monitor very large preproduction environments and large production environments that

- Span trust boundaries between domains and workgroups.
- Have multiple network environments segmented by firewalls.
- Have a need for high availability.
- Must have a scalable monitoring solution.

Ports Used

This configuration supports full distribution of features among servers in the management group as well as monitoring of devices across network boundaries, resulting in a longer list of ports that need to be available for communications. For more information, see [Connecting Management Groups in Operations Manager](#).

Distributed Deployment

You deploy either System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager in a distributed management group when you want to allow for scalability and high availability of your management servers and gateway servers. By default, all management servers are members of the All Management Servers Resource Pool, which balances the monitoring load of your management group as new management servers are added, and provides automatic failover for monitoring.

A distributed management group distributes the various features of Operations Manager across several servers. For example, you can install the operational database on one server, the web console on a second server, and the Reporting server on a separate server. This differs from the single-server management group installation, where all features are installed on one server. For more information, see [Single-Server Deployment of Operations Manager](#).

You can install a web console on a stand-alone server or on an existing management server, but you cannot install the management server feature on a server that has an existing web console. If you want to install the management server and web console on the same server, you must either install both features simultaneously, or install the management server before you install the web console.

This section of the Deployment Guide contains the following topics:

- [How to Install the First Management Server in a Management Group](#)
- [How to Install Additional Management Servers](#)
- [How to Install the Operations Console](#)
- [How to Configure the Operations Console to Use SSL When Connecting to a Reporting Server](#)
- [How to Install the Operations Manager Web Console](#)
- [Web Console Security in Operations Manager](#)
- [How to Install the Operations Manager Reporting Server](#)
- [Deploying a Gateway Server](#)
- [Deploying ACS and ACS Reporting](#)
- [Using SQL Server 2012 Always On Availability Groups with System Center 2012 SP1 - Operations Manager](#)

See Also

[Deploying System Center 2012 - Operations Manager](#)

How to Install the First Management Server in a Management Group

In System Center 2012 – Operations Manager, and System Center 2012 Service Pack 1 (SP1), Operations Manager the first feature that is installed is the management server. The operational database and data warehouse database are created during this setup. This procedure assumes that you have already installed a supported version of Microsoft SQL Server locally on the same server that you are going to install the first management server. However, you can specify an instance of SQL Server that is installed on a separate server.

You must ensure that your server meets the minimum system requirements for System Center 2012 – Operations Manager. For more information, see [System Requirements for System Center 2012 – Operations Manager](#).

Important

Before you follow these procedures, read the [Before You Begin](#) section of [Deploying System Center 2012 - Operations Manager](#).

To install the first management server in the management group

1. Log on to the server by using an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.

3. On the **Getting Started, Select features to install** page, select the **Management server** feature. You can also select any of the additional features listed. For example, to also install the Operations console, select **Operations console**. To read more about each feature and its requirements, click **Expand all**, or expand the buttons next to each feature, and then click **Next**.
4. On the **Getting Started, Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**. Or, type a new location or browse to one, and then click **Next**.
5. On the **Prerequisites** page, review and resolve any warnings or errors, and then click **Verify Prerequisites Again** to recheck the system.



Important

You might receive a message that indicates that ASP.NET 4 is not registered with Internet Information Services (IIS). To resolve this problem, open a Command Prompt window, select **Run as administrator**, and then run the following command:

```
%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r
```

6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration, Specify an installation option** page, select **Create the first Management server in a new management group**, type a name for your management group, and then click **Next**.



Note

After the management group name is set, it cannot be changed. The Management Group name cannot contain the following characters: , () ^ ~ : ; . ! ? " , ' ` @ # % \ / * + = \$ | & [] < > {}, and it cannot have a leading or trailing space. It is recommended that the Management Group name be unique within your organization if you plan to connect several management groups together.

8. On the **Configuration, Please read the license terms** page, review the Microsoft Software License Terms, select **I have read, understood and agree with the license terms**, and then click **Next**.
9. When the **Configuration, Configure the operational database** page opens, in the **Server name and instance name** box, type the name of the server and the name of the SQL Server instance for the database server that will host the operational database. If you installed SQL Server by using the default instance, you only have to type the server name. If you changed the default SQL Server port, you must type the new port number in the **SQL Server port** box.

As you type the values for the SQL Server and instance names, you see a red circle with a white **X** in it appear to the left of the **Server name and instance name** and **SQL Server port** boxes. The white **X** indicates that the values have not yet been validated, and the black text indicates that you have not entered any illegal characters. If you enter illegal characters, the text itself turns red.

The white **X** appears under the following circumstances:

- You entered an instance of SQL Server or a SQL Server port value that is not valid or that does not exist.
- The instance of SQL Server that you specified does not have the required configuration or features.
- You entered a value that is out-of-range (for example, port 999999).
- You entered an illegal character for that box (for example, server\instance%)

You can hover the cursor over the **Server name and instance name** text box to view additional information about the error.

10. After you type the correct value for the SQL Server database server name, click the **SQL Server port** box so that Setup will attempt to validate the values you typed for the SQL Server name and for the port number.
11. In the **Database name**, **Database size (MB)**, **Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.



Note

These paths do not change if you connect to a different instance of SQL Server.



Important

You might receive a message about having the wrong version of SQL Server, or you might encounter a problem with the SQL Server Windows Management Instrumentation (WMI) provider. To resolve this problem, open a Command Prompt window, select **Run as administrator**, and then run the following command. In the command, replace the *<path>* placeholder with the location of SQL Server.

```
mofcomp.exe "<path>\Microsoft SQL  
Server\100\Shared\sqlmgmproviderxpsp2up.mof".
```



Note

The SQL Server model database size must not be greater than 100 MB. If it is, you might encounter an error in Setup regarding the inability to create a database on SQL due to user permissions. To resolve the issue, you must reduce the size of the model database.

12. When the **Configuration, Configure the data warehouse database** page opens, in the **Server name and instance name** box, type the server name and the name of the instance of SQL Server for the database server that will host the data warehouse database.
13. Because this is the first management server installation, accept the default value of **Create a new data warehouse database**.
14. In the **Database name**, **Database size (MB)**, **Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.



Important


You might receive a message about having the wrong version of SQL Server, or you might encounter a problem with the SQL Server Windows Management Instrumentation (WMI) provider. To resolve this problem, open a Command Prompt window, select **Run as administrator**, and then run the following command. In the command, replace the *<path>* placeholder with the location of SQL Server.

mofcomp.exe “<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof”.

 **Note**

These paths do not change if you connect to a different instance of SQL Server.

15. On the **Configuration, Configure Operations Manager accounts** page, we recommend that you use the **Domain Account** option for the **Management server action account**, the **System Center Configuration service and System Center Data Access service** account, the **Data Reader account**, and the **Data Writer account**. None of them should have domain administrator credentials. Click **Next**.
16. On the **Configuration, Help improve System Center 2012 - Operations Manager** page, select your options, and then click **Next**.
17. If Windows Update is not enabled on the computer, the **Configuration, Microsoft Update** page appears. Select your options, and then click **Next**.
18. Review the options on the **Configuration, Installation Summary** page, and then click **Install**. Setup continues.
19. When Setup is finished, the **Setup is complete** page appears. Click **Close**.
20. Open the Operations console.
21. In the Operations console, in the navigation pane, click the **Administration** button, and then expand **Device Management**.
22. In **Device Management**, select **Management Servers**. In the results pane, you should see the management server that you just installed with a green check mark in the **Health State** column.

 **To install the first management server in the management group by using the Command Prompt window**

1. Log on to the server by using an account that has local administrative credentials.
2. Open the Command Prompt window by using the **Run as Administrator** option.

 **Note**

Setup.exe requires administrator privileges because the Setup process requires access to system processes that can only be used by a local administrator.

3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

 **Important**

The following command assumes that you specified the Local System for the

Management server action account (/UseLocalSystemActionAccount) and Data Access service (/UseLocalSystemDASAccount). To specify a domain/user name for these accounts, you must provide the following parameters instead.

```
/ActionAccountUser: <domain\username> /ActionAccountPassword: <password>
/DASAccountUser: <domain\username> /DASAccountPassword: <password>
setup.exe /silent /install /components:OMServer
/ManagementGroupName: "<ManagementGroupName>"
/SqlServerInstance: <server\instance>
/DatabaseName: <OperationalDatabaseName>
/DWSqlServerInstance: <server\instance>
/DWDatabaseName: <DWDatabaseName>
/UseLocalSystemActionAccount /UseLocalSystemDASAccount
/DatareaderUser: <domain\username>
/DatareaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
/EnableErrorReporting: [Never|Queued|Always]
/SendCEIPReports: [0|1]
/UseMicrosoftUpdate: [0|1]
/AcceptEndUserLicenseAgreement: [0|1]
```

See Also

[Distributed Deployment of Operations Manager](#)

How to Install Additional Management Servers

After you have installed System Center 2012 – Operations Manager, you can add additional management servers and join them to your existing management group.

Important

If you install a stand-alone web console on a server, you will not be able to add the management server feature to this server. If you want to install the management server and web console on the same server, you must either install both features simultaneously, or install the management server before you install the web console.

You must ensure that your server meets the minimum system requirements for System Center 2012 – Operations Manager. For more information, see [System Requirements for System Center 2012 – Operations Manager](#).

Important

Before you follow these procedures, read the [Before You Begin](#) section of [Deploying System Center 2012 - Operations Manager](#).

▶ **To install additional management servers**

1. Log on to the server with an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started, Select features to install** page, select **Management server**.
You can also additional features, such as the Operations console. Select **Operations console**. To read more about each feature and its requirements, click **Expand all**, or expand the buttons next to each feature, and then click **Next**.
4. On the **Getting Started, Select installation location** page, accept the default location of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one, and then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration, Specify an installation option** page, select **Add a Management server to an existing management group**, and then click **Next**.
8. When the **Configuration, Configure the operational database** page opens, type the name of the SQL Server database server and instance for the database server that hosts the operational database in the **Server name and instance name** box. If you installed SQL Server by using the default instance, you only have to enter the server name. If you changed the default SQL Server port, you must type in the new port number in the **SQL Server port** box.
As you type the values for SQL Server and instance name, you see a red circle with a white **X** in it appear to the left of the **Server name and instance name** and **SQL Server port** boxes. The white **X** indicates that the values have not yet been validated. The black text indicates that you have not entered any illegal characters. If you enter illegal characters, the text itself turns red.
9. After you have typed the correct values for the name of the SQL Server database server, click the **SQL Server port** box. Setup attempts to validate the values that you have typed for the SQL Server name and the port number.
10. Select the database name from the **Database name** drop-down list, and then click **Next**.
11. On the **Configuration, Configure Operations Manager accounts** page, we recommend that you use the **Domain Account** option for the **Management server action account** and the **System Center Configuration service and System Center Data Access service** account. Neither of them should have domain administrator credentials. Click **Next**.



You must provide the same credentials for the Management server action account and the System Center Configuration Service and System Center Data Access service that you provided when you created the first management server in your management group.

12. If Windows Update is not enabled on the computer, the **Configuration, Microsoft Update** page appears. Select your options, and then click **Next**.
13. Review the options on the **Configuration, Installation Summary** page, and then click **Install**. Setup continues.
14. When setup is finished, the **Setup is complete** page appears. Click **Close**.
15. Open the Operations console.
16. In the Operations console, select the **Administration** workspace, and then expand **Device Management**.
17. In **Device Management**, select **Management Servers**. In the results pane, you should see the management server that you just installed with a green check mark in the **Health State** column.

► **To install additional management servers by using the Command Prompt window**

1. Log on to the server by using an account that has local administrative credentials.
2. Open the Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

 **Important**

The following command assumes that you specified the Local System for the Management server action account (`/UseLocalSystemActionAccount`) and Data Access service (`/UseLocalSystemDASAccount`). To specify a domain/user name for these accounts, you must provide the following parameters instead.

```
/ActionAccountUser: <domain\username> /ActionAccountPassword: <password>
/DASAccountUser: <domain\username> /DASAccountPassword: <password>
setup.exe /silent /install /components:OMServer
/SqlServerInstance: <server\instance>
/DatabaseName: <OperationalDatabaseName>
/UseLocalSystemActionAccount /UseLocalSystemDASAccount
/DataReaderUser: <domain\username>
/DataReaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
/EnableErrorReporting: [Never|Queued|Always]
/SendCEIPReports: [0|1]
```


/UseMicrosoftUpdate: [0|1]

See Also

[Distributed Deployment of Operations Manager](#)

How to Install the Operations Console

After you install System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager, you can install the Operations console on other servers and computers. For example, you might want to view monitoring data from your desktop computer. Before you install an System Center 2012 – Operations Manager Operations console, you must install [Microsoft .NET Framework 3.5 SP1 hotfix](#).

You must ensure that the computer that will host the Operations console meets the minimum system requirements. For more information, see [System Requirements for System Center 2012 – Operations Manager](#).

Important

Before you follow these procedures, read the [Before You Begin](#) section of [Deploying System Center 2012 - Operations Manager](#).

To install the Operations console

1. Log on to the computer that will host the Operations console with an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started, Select features to install** page, select **Operations console**. To read more about what each feature provides and its requirements, click **Expand all**, or expand the buttons next to each feature, and then click **Next**.
4. On the **Getting Started, Select installation location** page, accept the default location of **C:\Program Files\System Center 2012\Operations Manager**, or type a new location or browse to one, and then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again**.
6. If the Prerequisite checker returns no warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration, Help improve System Center - Operations Manager** page, select your options, and then click **Next**.
8. If Windows Update is not enabled on the computer, the **Configuration, Microsoft Update** page appears. Select your options, and then click **Next**.
9. Review the options on the **Configuration, Installation Summary** page, and then click **Install**. Setup continues.
10. When Setup is finished, the **Setup is complete** page appears. Click **Close**, and the Operations console opens.
11. In the Operations console, on the **Connect to Server** page, type the name of the first

management server that you installed in the management group in the **Server name** box, and then click **Connect**.

 **Important**

If you are going to edit company knowledge on this computer, you also have to install the [Microsoft Visual Studio 2005 Tools for Office Second Edition Runtime](#).

 **Important**

Company knowledge cannot be edited with the x64 version of Microsoft Word 2010. You must install the x86 version of Microsoft Office 2010 or an earlier version to edit knowledge.

 **To install the Operations console by using the Command Prompt window**

1. Log on to the server by using an account that has local administrative credentials.
2. Open the Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

```
setup.exe /silent /install /components:OMConsole  
/EnableErrorReporting:[Never|Queued|Always]  
/SendCEIPReports:[0|1] /UseMicrosoftUpdate: [0|1]
```

See Also

[Distributed Deployment of Operations Manager](#)

How to Configure the Operations Console to Use SSL When Connecting to a Reporting Server

Before you can configure the Operations Manager Operations console to use SSL when connecting to a Reporting Server, you must first install an SSL certificate on IIS. You then configure the Operations console to use SSL.

On the Reporting Server, start Internet Information Services (IIS) Manager to request and install an SSL certificate. For more information about how to implement SSL in IIS, see the Knowledge Base article [How to implement SSL in IIS](#).

Use the following procedure to configure the Operations console to use SSL.

 **To configure the Operations Console to use SSL**

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.

 **Note**

When you run the Operations console on a computer that is not a management

server, the **Connect To Server** dialog box displays. In the **Server name** text box, type the name of the Operations Manager management server that you want the Operations console to connect to.

3. In the Administration pane, expand **Administration**, expand **Device Management**, and then click **Settings**.
4. In the Settings pane, right-click **Reporting**, and then click **Properties**.
5. In the **General** tab, under **Reporting Server Settings**, click the **Reporting server URL** drop-down list and select **https://**.
6. Edit the URL by replacing **:80** with **:443**, and then click **OK**.

See Also

[Distributed Deployment of Operations Manager](#)

How to Install the Operations Manager Web Console

You can install the web console when you install Operations Manager, or you can install it separately. You can install a stand-alone web console or install it on an existing management server that meets the prerequisites. For information about the prerequisites, see [System Requirements for System Center 2012 – Operations Manager](#). After you install the web console, you must configure permissions inheritance to allow users to view performance and diagram views. For instructions, see [To configure permissions inheritance for the web console](#).

Important

If you install a stand-alone web console on a server, you will not be able to add the management server feature to this server. If you want to install the management server and web console on the same server, you must either install both features simultaneously, or install the management server before you install the web console.

When you install the web console, three components are installed: the Operations Manager web console itself, Application Diagnostics console, and Application Advisor console.

Note

If Application Diagnostics console is not installed, when viewing APM alerts, you will not be able to use the link embedded in the alert description to launch the APM event details.

To use this feature, install the web console within the management group.

If you plan to use network load balancing with Application Diagnostics console and Application Advisor console, be sure to use sticky sessions. This ensures that the same instance of the console is used for the entire session. For more information about network load balancing, see [Network Load Balancing](#). For more information about sessions, see [Support for Sessions](#).

Security

The web console operates with sensitive data, such as clear text user credentials, server names, IP addresses, and so on. If these are exposed on the network, they can represent a significant security risk. If Internet Information Services (IIS) does not have Secure Sockets Layer (SSL) configured, you are advised to configure it manually.

Important

Before you follow these procedures, read the [Before You Begin](#) section of [Deploying System Center 2012 - Operations Manager](#).

If the web console does not have sufficient access to the operational database or the data warehouse database, you will receive a warning during the web console configuration step. You can proceed with Setup, but the web console will not be configured correctly for .NET Application monitoring. To resolve this issue, you can have your database administrator run the following SQL Server statement on both the operational database and data warehouse database:

```
EXEC [apm].GrantRWPermissionsToComputer N'[LOGIN]'
```

The local and remote parameters are as follows:

- For local installation, the LOGIN is: IIS APPPOOL\OperationsManagerAppMonitoring
- For remote installation, the LOGIN is: Domain\MachineName\$

Note

If you run **Repair** on the web console after installation, the settings that were selected during installation will be restored. Any changes that you manually make to the web console configuration after the installation will be reset.

To install a stand-alone web console

1. Log on to the computer that will host the web console with an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started, Select features to install** page, select **Web console**. To read more about what each feature provides and its requirements, click **Expand all**, or expand the buttons next to each feature, and then click **Next**.
4. On the **Getting Started, Select installation location** page, accept the default location of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one, and then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.

Note

Installation of the web console requires that ISAPI and CGI Restrictions in IIS be enabled for ASP.NET 4. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET v4.0.30319**, and then click **Allow**.

Important

You must install IIS before installing .NET Framework 4. If you installed IIS after installing .NET Framework 4, you must register ASP.NET 4.0 with IIS. Open a Command prompt window by using the **Run As Administrator** option and then

run the following command:

```
%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r
```

6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration, Specify a management server** page, enter the name of a management server that only the web console uses, and then click **Next**.
8. On the **Configuration, Specify a web site for use with the Web console** page, select the **Default Web Site**, or the name of an existing website. Select **Enable SSL** only if the website has been configured to use Secure Sockets Layer (SSL), and then click **Next**.

 **Warning**

Installing the web console on a computer that has SharePoint installed is not supported.

9. On the **Configuration, Select an authentication mode for use with the Web console** page, select your options, and then click **Next**.

 **Note**

If you install the management server on a server using a domain account for System Center Configuration service and System Center Data Access service, and then install the web console on a different server and select Mixed Authentication, you may need to register [Service Principal Names](#) and configure constraint delegations, as described in [Running the Web Console Server on a standalone server using Windows Authentication](#).

10. If Microsoft Update is not enabled on the computer, the **Configuration, Microsoft Update** page appears. Select your options, and then click **Next**.
11. Review your selections on the **Configuration, Installation Summary** page, and then click **Install**. Setup continues.
12. When Setup is finished, the **Setup is complete** page appears. Click **Close**.

 **To install the web console on an existing management server**

1. Log on to the computer that is hosting a management server with an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started, What do you want to do?** page, click **Add a feature**.
4. On the **Getting Started, Select features to install** page, select **Web console**, and then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors, and then click **Verify Prerequisites Again** to recheck the system.

 **Note**

Installation of the web console requires that ISAPI and CGI Restrictions in IIS be enabled for ASP.NET 4. To enable this, select the web server in IIS Manager, and then double-click **ISAPI and CGI Restrictions**. Select **ASP.NET**

v4.0.30319, and then click **Allow**.

 **Important**

You must install IIS before installing .NET Framework 4. If you installed IIS after installing .NET Framework 4, you must register ASP.NET 4.0 with IIS. Open a Command prompt window by using the **Run As Administrator** option and then run the following command:

```
%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -r
```

6. If the Prerequisite checker returns no warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration, Specify a web site for use with the Web console** page, select the **Default Web Site**, or the name of an existing website. Select **Enable SSL** only if the website has been configured to use Secure Sockets Layer (SSL), and then click **Next**.
8. On the **Configuration, Select an authentication mode for use with the Web console** page, select your options, and then click **Next**.
9. If Windows Update is not activated on the computer, the **Configuration, Microsoft Update** page appears. Select your options, and then click **Next**.
10. Review your selections on the **Configuration, Installation Summary** page, and click **Install**. Setup continues.
11. On the **Setup is complete** page, click **Close**.

 **Important**

The Default website must have an http or https binding configured.

 **To install a web console by using the Command Prompt window**

1. Log on to the computer with an account that has local administrative credentials.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.

 **Important**

Use the `/WebConsoleSSL` parameter only if your website has Secure Sockets Layer (SSL) activated.

For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.

 **Note**

The `/ManagementServer` parameter is only required when you are installing the web console on a server that is not a management server.

```
setup.exe /silent /install /components:OMWebConsole  
/ManagementServer: <ManagementServerName>  
/WebSiteName: "<WebSiteName>" [/WebConsoleUseSSL]
```

```
/WebConsoleAuthorizationMode: [Mixed|Network]
/UseMicrosoftUpdate: [0|1]
```

► To configure permissions inheritance for the web console

1. In Windows Explorer, navigate to the MonitoringView folder in the installation directory for the web console (by default, C:\Program Files\System Center 2012\Operations Manager\WebConsole\MonitoringView), right-click the TemplImages folder, and click **Properties**.
2. On the **Security** tab, click **Advanced**.
3. On the **Permissions** tab, click **Change Permissions**.
4. Select the **Include inheritable permissions from this object's parent** checkbox.
5. In **Permission entries**, click **Administrators**, and then click **Remove**. Repeat for the **SYSTEM** entry, and then click **OK**.
6. Click **OK** to close **Advanced Security Settings for TemplImages**, and then click **OK** to close **TemplImages Properties**.

All information and content at

<http://blogs.technet.com/b/momteam/archive/2008/01/31/running-the-web-console-server-on-a-standalone-server-using-windows-authentication.aspx> is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied or statutory, as to the information at this website.

See Also

[Distributed Deployment of Operations Manager](#)

Web Console Security in Operations Manager

The web console server provides a browser-based alternative to the Monitoring pane of the Operations Manager Operations console. The web console server is commonly used when you want to access Operations Manager management group monitoring data in the following ways:

- From the Internet
- Without installing the Operations console
- From a location with low-bandwidth connectivity
- When notifications are configured to contain hyperlinks to the relevant alerts in the web console

When you install the web console, you must specify a web site for use with the web console. The default port for accessing the web console from a browser using Windows-based authentication is the same port as the web site that is selected when the web console was installed. If the web site chosen has been configured to use Secure Sockets Layer (SSL), then you must also select **Enable SSL**.

You must also select an authentication mode for use with the web console. Use mixed authentication for intranet scenarios and network authentication for extranet scenarios.



Note

The best practice for accessing the web console from the Internet is to use network authentication with SSL with the web console.

The web console uses two encryption algorithms:

1. SHA256
2. HMACSHA256

These algorithms may not be sufficient to meet compliance standards. For instance, they do not meet the Federal Information Processing Standard (FIPS). In order to meet a compliance standard, you need to map these names, in the appropriate configuration files, to appropriate encryption algorithms.

The next section uses FIPS compliant algorithms as an example.

How to Use FIPS Compliant Algorithms

System Center 2012 – Operations Manager can use Federal Information Processing Standard (FIPS) compliant algorithms. A FIPS compliant algorithm is included on your installation media. After you install it, you need to manually edit several configuration files.

In order to use algorithms that are FIPS compliant, follow these steps for all Operations Manager server components.

- Install Microsoft.EnterpriseManagement.Cryptography.dll.
- Edit several instances of the machine.config file.

For systems that host a web console, also do the following steps.

- Edit the WebHost\web.config file.
- Edit the MonitoringView\web.config file.

You need the Global Assembly Cache Tool, gacutil.exe. This utility is part of the Windows SDK. For more information, see [Gacutil.exe \(Global Assembly Cache Tool\)](#).

▶ To install the cryptography DLL

1. On the system hosting the web console, use the **Run as Administrator** option to open a Command Prompt window.
2. Change directories to the SupportTools directory of your installation media, and then change directory as appropriate to your platform: AMD64 or i386.
3. Run the following gacutil command:

```
gacutil.exe -i  
Microsoft.EnterpriseManagement.Cryptography.dll
```

▶ To edit the machine.config files

1. Use a plain text editor to open the following machine.config file:
%WinDir%\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

2. Add the following content:

```
<mscorlib>
  <cryptographySettings>
    <cryptoNameMapping>
      <cryptoClasses>
        <cryptoClass
SHA256CSP="System.Security.Cryptography.SHA256CryptoServicePr
vider, System.Core, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089"/>
        <cryptoClass HMACSHA256CSP
="Microsoft.EnterpriseManagement.Cryptography.HMACSHA256,
Microsoft.EnterpriseManagement.Cryptography,
Version=7.0.5000.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35"/>
      </cryptoClasses>
      <nameEntry name="SHA256" class="SHA256CSP"/>
      <nameEntry name="HMACSHA256"
class="HMACSHA256CSP"/>
    </cryptoNameMapping>
  </cryptographySettings>
</mscorlib>
```

Save and close the file when finished.

3. Repeat the preceding step on the following files:

%WinDir%\Microsoft.NET\Framework\v4.0.30319\Config\machine.config

%WinDir%\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config

▶ To edit the web.config file in WebHost

1. Use a plain text editor to open the following web.config file:

C:\Program Files\System Center 2012\Operations
Manager\WebConsole\WebHost\web.config

2. In the <encryption> element, add the following element:

```
<symmetricAlgorithm iv="SHA256"/>
```

3. In the <connection autoSignIn="true" autoSignOutInterval="30"> element, in the <session> tag, add the following attribute: tokenAlgorithm="SHA256".

```
<connection autoSignIn="True" autoSignOutInterval="30">
<session encryptionKey="SessionEncryptionKey"
tokenAlgorithm="SHA256">
```

4. Save and close the file.

► To edit the web.config file in MonitoringView

1. Use a plain text editor to open the following web.config file:

```
C:\Program Files\System Center 2012\Operations
Manager\WebConsole\MonitoringView\web.config
```

2. In the <encryption> element, add the following element:

```
<symmetricAlgorithm iv="SHA256"/>
```

3. In the <connection autoSignIn="true" autoSignOutInterval="30"> element, in the <session> tag, add the following attribute: tokenAlgorithm="SHA256".

```
<connection autoSignIn="True" autoSignOutInterval="30">
<session encryptionKey="SessionEncryptionKey"
tokenAlgorithm="SHA256">
```

4. In the <system.web> element, add the following element:

```
<machineKey validationKey="AutoGenerate,IsolateApps"
decryptionKey="AutoGenerate,IsolateApps" validation="3DES"
decryption="3DES"/>
```

5. Save and close the file.

How to Install the Operations Manager Reporting Server

In this procedure, the Reporting server is installed on a stand-alone server that is hosting the SQL Server database and SQL Server Reporting Services.

Warning

Although SQL Server Reporting Services is installed on the stand-alone server, Operations Manager reports are not accessed on this server; instead, they are accessed in the **Reporting** workspace in the Operations console. If you want to access published reports via the web console, you must install the Operations Manager web console on the same computer as Operations Manager Reporting server.

You must ensure that your server meets the minimum system requirement for Operations Manager. For more information, see [System Requirements for System Center 2012 – Operations Manager](#).

Important

Before you follow these procedures, read the [Before You Begin](#) section of [Deploying System Center 2012 - Operations Manager](#).

Installing Operations Manager Reporting

No other applications that are using SQL Server Reporting Services can be installed on this instance of SQL Server.

Ensure that SQL Server Reporting Services has been correctly installed and configured. For more information about how to install and configure SQL Server Reporting Services, see [SQL Server Installation \(SQL Server 2012 R2\)](#).

Note

Before you continue with this procedure, ensure that the account you plan to use for the Data Warehouse Write account has SQL Server logon rights and is an Administrator on the computers hosting both the operational database and the Reporting data warehouse database. Otherwise, Setup fails, and all changes are rolled back, which might leave SQL Server Reporting Services in an inoperable state.

To verify that Reporting Services is configured correctly

1. Verify that the **ReportServer** and **ReportServerTempDB** databases in SQL Server Management Studio are located on the stand-alone server. Click **Start**, point to **All Programs**, point to **Microsoft SQL Server 2008 R2**, point to **SQL Server Management Studio**, and then connect to the default database instance. Open the **Databases** node and verify that the two Reporting Services databases exist under this node.
2. Verify the correct configuration of SQL Server Reporting Services. Click **Start**, point to **Programs**, point to the appropriate offering of Microsoft SQL Server, point to **Configuration Tools**, and then click **Reporting Services Configuration Manager**. Connect to the instance on which you installed Reporting Services.
3. In the navigation pane, select the <servername>\SQLinstance. This displays the Report Server status in the results pane. Ensure that the **Report Server Status** is **Started**.
4. In the navigation pane, select **Scale-out Deployment**, and then ensure that the **Status** column has the value of **Joined**.
5. If **Report Server** is not started and the **Scale out Deployment** is not joined, check the configuration of **Service Account**, **Web Service URL**, and **Database**.
6. Confirm that the SQL Server Reporting Services service is running. On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Services**.
7. In the **Name** column, find the **SQL Server Reporting Services** instance service and verify that its status reads **Started** and that the **Startup Type** is **Automatic**.
8. In the **Name** column, find the **SQL Server Agent** service and verify that its status reads **Started** and that its **Startup Type** is **Automatic**.
9. Verify that the Report Server website is functioning and available by browsing to **http://servername/reportserver<\$instance>**. You should see a page with the

<servername>/ReportServer<\$INSTANCE> and the text, **Microsoft SQL Server Reporting Services Version ###.###.###.##** where the # is the version number of your SQL Server installation.

10. Verify that the Report Manager website is configured correctly by opening **Internet Explorer** and browsing to **http://<servername>/reports<instance>**.
11. In the Report Manager website, click **New Folder** to create a new folder. Enter a name and description, and then click **OK**. Ensure that the new, created folder is visible on the Report Manager website.

▶ To install Operations Manager Reporting

1. Log on to the computer with an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started, Select features to install** page, select the **Reporting server** feature. To read more about each feature and its requirements, click **Expand all**, or expand the buttons next to each feature, and then click **Next**.
4. On the **Getting Started, Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager** or type a new location or browse to one, and then click **Next**.
5. On the **Prerequisites** page, review and resolve any warnings or errors, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, continue to the **Prerequisites, Proceed with Setup** page. Click **Next**.
7. On the **Configuration, Specify a Management server** page, enter the name of a management server that is used by the Reporting features only. Then click **Next**.
8. On the **Configuration, SQL Server instance for reporting services** page, select the instance of SQL Server that hosts SQL Server Reporting Services, and then click **Next**.
9. On the **Configuration, Configure Operations Manager accounts** page, enter the credentials for the **Data Reader account**, and then click **Next**.
10. On the **Configuration, Help improve System Center - Operations Manager** page, select your options, and then click **Next**.
11. If Windows Update is not activated on the computer, the **Configuration, Microsoft Update** page appears. Select your options, and then click **Next**.
12. Review the options on the **Configuration, Installation Summary** page, and then click **Install**. Setup continues.
13. When Setup is finished, the **Setup is complete** page appears. Click **Close**.

▶ To install Operations Manager Reporting by using the Command Prompt window

1. Log on to the server by using an account that has local administrative credentials.
2. Open the Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.



Note

The /ManagementServer parameter is only required when you are installing reporting on a server that is not a management server.

```
setup.exe /silent /install /components:OMReporting  
/ManagementServer: "<ManagementServerName>"  
/SRSInstance: <server\instance>  
/DataReaderUser: <domain\username>  
/DataReaderPassword: <password>  
/SendODRReports: [0|1]  
/UseMicrosoftUpdate: [0|1]
```

► To confirm the health of Operations Manager reports

1. Open the Operations console, and select the **Reporting** workspace.



Note

After initial deployment, reports can require up to 30 minutes to appear.

2. Click **Microsoft ODR Report Library**, and then double-click any of the reports listed. The selected report is then generated and displayed in a new window.

By default, you should see the following reports:

- **Alerts Per Day**
 - **Instance Space**
 - **Management Group**
 - **Management Packs**
 - **Most Common Alerts**
3. Close the report window.

See Also

[Distributed Deployment of Operations Manager](#)

Deploying a Gateway Server

Gateway servers are used to enable agent-management of computers that are outside the Kerberos trust boundary of management groups, such as in a domain that is not trusted. The gateway server acts as a concentration point for agent-to-management server communication. Agents in domains that are not trusted communicate with the gateway server and the gateway server communicates with one or more management servers. Because communication between the gateway server and the management servers occurs over only one port (TCP 5723), that port is the only one that has to be opened on any intervening firewalls to enable management of multiple agent-managed computers. Multiple gateway servers can be placed in a single domain so that the agents can failover from one to the other if they lose communication with one of the

gateway servers. Similarly, a single gateway server can be configured to failover between management servers so that no single point of failure exists in the communication chain.

Because the gateway server resides in a domain that is not trusted by the domain that the management group is in, certificates must be used to establish each computer's identity, agent, gateway server, and management server. This arrangement satisfies the requirement of Operations Manager for mutual authentication.

Deploying a gateway topics

- [How to Deploy a Gateway Server](#)
- [How to Chain Gateways](#)

How to Deploy a Gateway Server

To monitor computers that lie outside the trust boundary of a management server without the use of a gateway server, you need to install and manually maintain certificates on the management servers and the computers to be monitored. When this configuration is used instead of using a gateway server, additional ports must be opened for agent-to-management server communication. For a listing of all ports that are necessary, see [System Requirements for System Center 2012 – Operations Manager](#).

► Procedure overview

1. Request certificates for any computer in the agent, gateway server, management server chain.
2. Import those certificates into the target computers by using the MOMCertImport.exe tool.
3. Distribute the Microsoft.EnterpriseManagement.GatewayApprovalTool.exe to the management server.
4. Run the Microsoft.EnterpriseManagement.GatewayApprovalTool.exe tool to initiate communication between the management server and the gateway
5. Install the gateway server.

Preparing for Installation

► Before You Start

1. Deployment of gateway servers requires certificates. You need to have access to a certification authority (CA). This can be a public CA such as VeriSign, or you can use Microsoft Certificate Services. This procedure provides the steps to request, obtain, and import a certificate from Microsoft Certificate Services.
2. Reliable name resolution must exist between the agent-managed computers and the gateway server and between the gateway server and the management servers. This name resolution is typically done through DNS. However, if it is not possible to get proper name resolution through DNS, it might be necessary to manually create entries in each computer's hosts file.



Note

The hosts file is located in the \Windows\system32\drivers\ directory, and it contains directions for configuration.

Obtaining Computer Certificates from Microsoft Certificate Services

For more information, see [Authentication and Data Encryption for Windows Computers](#).

Distributing the Microsoft.EnterpriseManagement.GatewayApprovalTool

The Microsoft.EnterpriseManagement.GatewayApprovalTool.exe tool is needed only on the management server, and it only has to be run once.

▶ To copy Microsoft.EnterpriseManagement.GatewayApprovalTool.exe to management servers

1. From a target management server, open the Operations Manager installation media \SupportTools directory.
2. Copy the Microsoft.EnterpriseManagement.GatewayApprovalTool.exe from the installation media to the Operations Manager installation directory.

Registering the Gateway with the Management Group

This procedure registers the gateway server with the management group, and when this is completed, the gateway server appears in the Discovered Inventory view of the management group.

▶ To run the gateway Approval tool

1. On the management server that was targeted during the gateway server installation, log on with the Operations Manager Administrator account.
2. Open a command prompt, and navigate to the Operations Manager installation directory or to the directory that you copied the Microsoft.EnterpriseManagement.gatewayApprovalTool.exe to.
3. At the command prompt, run `Microsoft.EnterpriseManagement.gatewayApprovalTool.exe /ManagementServerName=<managementserverFQDN> /GatewayName=<GatewayFQDN> /Action=Create`
4. If the approval is successful, you will see `The approval of server <GatewayFQDN> completed successfully.`
5. If you need to remove the gateway server from the management group, run the same command, but substitute the `/Action=Delete` flag for the `/Action=Create` flag.
6. Open the Operations console to the Monitoring view. Select the Discovered Inventory view to see that the gateway server is present.

Installing Gateway Server

This procedure installs the gateway server. The server that is to be the gateway server should be a member of the same domain as the agent-managed computers that will be reporting to it.



Tip

An installation will fail when starting Windows Installer (for example, installing a gateway server by double-clicking MOMGateway.msi) if the local security policy User Account Control: Run all administrators in Admin Approval Mode is enabled.

▶ **To run Operations Manager Gateway Windows Installer from a Command Prompt window**

1. On the Windows desktop, click **Start**, point to **Programs**, point to **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. In the **Administrator: Command Prompt** window, navigate to the local drive that hosts the Operations Manager installation media.
3. Navigate to the directory where the .msi file is located, type the name of the .msi file, and then press ENTER.

▶ **To install the gateway server**

1. Log on to the gateway server with Administrator rights.
2. From the Operations Manager installation media, start **Setup.exe**.
3. In the **Install** area, click the **Gateway management server** link.
4. On the **Welcome** screen, click **Next**.
5. On the **Destination Folder** page, accept the default, or click **Change** to select a different installation directory, and then click **Next**.
6. On the **Management Group Configuration** page, type the target management group name in the **Management Group Name** field, type the target management server name in the **Management Server** field, check that the **Management Server Port** field is **5723**, and then click **Next**. This port can be changed if you have enabled a different port for management server communication in the Operations console.
7. On the **Gateway Action Account** page, select the **Local System** account option, unless you have specifically created a domain-based or local computer-based gateway Action account. Click **Next**.
8. On the **Microsoft Update** page, optionally indicate if you want to use Microsoft Update, and then click **Next**.
9. On the **Ready to Install** page, click **Install**.
10. On the **Completing** page, click **Finish**.

▶ **To install the gateway server by using the Command Prompt window**

1. Log on to the gateway server with Administrator rights.
2. Open the Command Prompt window by using the **Run as Administrator** option.
3. Run the following command, where *path\Directory* is the location of the Momgateway.msi, and *path\Logs* is the location where you want to save the log file. Momgateway.msi can be found in the Operations Manager installation media.

```
%WinDir%\System32\msiexec.exe /i  
path\Directory\MOMGateway.msi /qn /l*v
```



```
path\Logs\GatewayInstall.log
ADDLOCAL=MOMGateway
MANAGEMENT_GROUP=""
IS_ROOT_HEALTH_SERVER=0
ROOT_MANAGEMENT_SERVER_AD=<ParentMSFQDN>
ROOT_MANAGEMENT_SERVER_DNS=<ParentMSFQDN>
ACTIONS_USE_COMPUTER_ACCOUNT=0
ACTIONS_DOMAIN=<DomainName>
ACTIONS_USER=<ActionAccountName>
ACTIONS_PASSWORD=<Password>
ROOT_MANAGEMENT_SERVER_PORT=5723
[INSTALLDIR=<path\Directory>]
```

Importing Certificates with the MOMCertImport.exe Tool

Perform this operation on each gateway server, management server, and computer that will be agent-managed and that is in a domain that is not trusted.

► To import computer certificates by using MOMCertImport.exe

1. Copy the MOMCertImport.exe tool from the installation media \SupportTools\<platform> (x86 or ia64) directory to the root of the target server or to the Operations Manager installation directory if the target server is a management server.
2. As an administrator, open a Command Prompt window and change the directory to the directory where MOMCertImport.exe is, and then run `momcertimport.exe /SubjectName <certificate subject name>`. This makes the certificate usable by Operations Manager.

Configuring Gateway Servers for Failover Between Management Servers

Although gateway servers can communicate with any management server in the management group, this must be configured. In this scenario, the secondary management servers are identified as targets for gateway server failover.

Use the `Set-ManagementServer-gatewayManagementServer` command in Operations Manager Shell, as shown in the following example, to configure a gateway server to failover to multiple management servers. The commands can be run from any Command Shell in the management group.

► To configure gateway server failover between management servers

1. Log on to the management server with an account that is a member of the Administrators role for the management group.
2. On the Windows desktop, click **Start**, point to **Programs**, point to **System Center**

Operations Manager, and then click **Command Shell**.

3. In Command Shell, follow the example that is described in the next section.

Description

The following example can be used to configure gateway server failover to multiple management servers.

Code

```
$GatewayServer = Get-SCOMGatewayManagementServer -Name "ComputerName.Contoso.com"
$FailoverServer = Get-SCOMManagementServer -Name
"ManagementServer.Contoso.com", "ManagementServer2.Contoso.com"
Set-SCOMParentManagementServer -GatewayServer $GatewayServer -FailoverServer
$FailoverServer
```

See Also

[Deploying a Gateway Server](#)

How to Chain Gateways

It is sometimes necessary to chain multiple gateways together in order to monitor across multiple untrusted boundaries. This topic describes how to chain multiple gateways together.



Note

You should install one gateway at a time and verify that each newly installed gateway is configured correctly before adding another gateway in the chain.

▶ To chain multiple gateway servers

1. On the management server that was targeted during the gateway server installation, run the `Microsoft.EnterpriseManagement.GatewayApprovalTool.exe` tool to initiate communication between the management server and the gateway.
2. Open a command prompt, and navigate to the Operations Manager installation directory or, and then run the following: `Microsoft.EnterpriseManagement.gatewayApprovalTool.exe /ManagementServerName=<managementserverFQDN> /GatewayName=<GatewayFQDN> /Action=Create`
3. Install the gateway server on a new server. For more information, see [Installing Gateway Server](#).
4. Configure the certificates between gateways in the same way that you would configure certificates between a gateway and a management server. For more information, see [Importing Certificates with the MOMCertImport.exe Tool](#). The Health Service can only load and use a single certificate. Therefore, the same certificate is used by the parent and child of the gateway in the chain.

See Also

[Deploying a Gateway Server](#)

Authentication and Data Encryption for Windows Computers

System Center 2012 – Operations Manager consists of features such as the management server, gateway server, Reporting server, Operational database, Reporting data warehouse, agent, web console, and Operations console. This section explains how authentication is performed and identifies connection channels where the data is encrypted.

Certificate-Based Authentication

When an Operations Manager agent and management server are separated by either an untrusted forest or workgroup boundary, certificate-based authentication will need to be implemented. The following sections provide information about these situations and specific procedures for obtaining and installing certificates from Windows-based certification authorities.

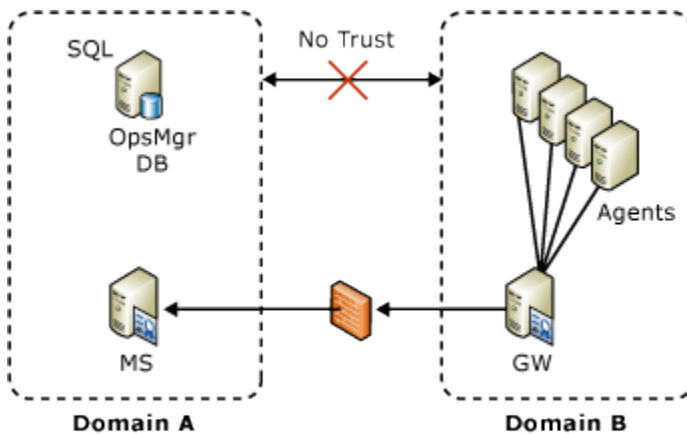
Setting Up Communication Between Agents and Management Servers Within the Same Trust Boundary

An agent and the management server use Windows authentication to mutually authenticate with each other before the management server accepts data from the agent. The Kerberos version 5 protocol is the default method for providing authentication. In order for Kerberos-based mutual authentication to function, the agents and management server must be installed in an Active Directory domain. If an agent and a management server are in separate domains, full trust must exist between the domains. In this scenario, after mutual authentication has taken place, the data channel between the agent and the management server is encrypted. No user intervention is required for authentication and encryption to take place.

Setting Up Communication Between Agents and Management Servers Across Trust Boundaries

An agent (or agents) might be deployed into a domain (domain B) separate from the management server (domain A), and no two-way trust might exist between the domains. Because there is no trust between the two domains, the agents in one domain cannot authenticate with the management server in the other domain using the Kerberos protocol. Mutual authentication between the Operations Manager features within each domain still occurs.

A solution to this situation is to install a gateway server in the same domain where the agents reside, and then install certificates on the gateway server and the management server to achieve mutual authentication and data encryption. The use of the gateway server means you need only one certificate in domain B and only one port through the firewall, as shown in the following illustration.



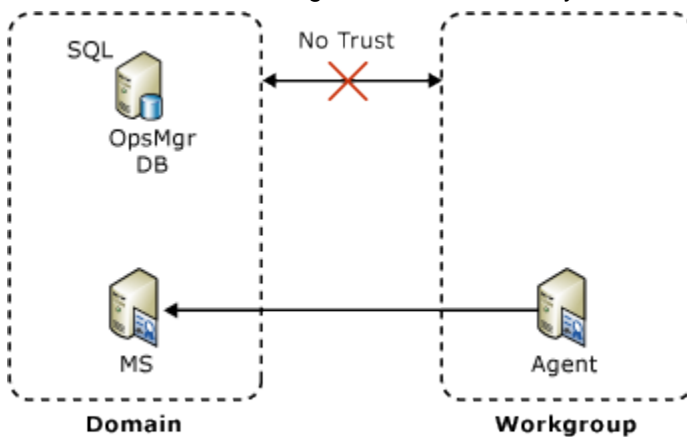
Setting Up Communication Across a Domain – Workgroup Boundary

In your environment, you may have one or two agents deployed to a workgroup inside your firewall. The agent in the workgroup cannot authenticate with the management server in the domain using the Kerberos protocol. A solution to this situation is to install certificates on both the computer hosting the agent and the management server that the agent connects to, as shown in the following illustration.



Note

In this scenario, the agent must be manually installed.



Perform the following steps on both the computer hosting the agent and the management server using the same certification authority (CA) for each:

- Request certificates from the CA.
- Approve the certificate requests on the CA.
- Install the approved certificates in the computer certificate stores.
- Use the MOMCertImport tool to configure Operations Manager.

These are the same steps for installing certificates on a gateway server, except you do not install or run the gateway approval tool.

Confirming Certificate Installation

If you have properly installed the certificate, the following event is written into the Operations Manager event log.

Type	Source	Event ID	General
Information	OpsMgr Connector	20053	The OpsMgr Connector has loaded the specified authentication certificate successfully.

During the setup of a certificate, you run the MOMCertImport tool. When the MOMCertImport tool has finished, the serial number of the certificate that you imported is written to the registry at the following subkey.

Caution

Incorrectly editing the registry can severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Machine Settings

Authentication and Data Encryption Between Management Server, Gateway Server, and Agents

Communication among these Operations Manager features begins with mutual authentication. If certificates are present on both ends of the communications channel, then certificates will be used for mutual authentication; otherwise, the Kerberos version 5 protocol is used. If any two features are separated across an untrusted domain, mutual authentication must be performed using certificates.

Normal communications, such as events, alerts, and deployment of a management pack, occur over this channel. The previous illustration shows an example of an alert being generated on one of the agents that is routed to the management server. From the agent to the gateway server, the Kerberos security package is used to encrypt the data, because the gateway server and the agent are in the same domain. The alert is decrypted by the gateway server and re-encrypted using certificates for the management server. After the management server receives the alert, the management server decrypts the message, re-encrypts it using the Kerberos protocol, and sends it to the management server where the management server decrypts the alert.

Some communication between the management server and the agent may include credential information; for example, configuration data and tasks. The data channel between the agent and the management server adds another layer of encryption in addition to the normal channel encryption. No user intervention is required.

Management Server and Operations Console, Web Console Server, and Reporting Server

Authentication and data encryption between the management server and the Operations console, web console server, or Reporting Server is accomplished by using Windows Communication

Foundation (WCF) technology. The initial attempt at authentication is made by using the user's credentials. The Kerberos protocol is attempted first. If the Kerberos protocol does not work, another attempt is made using NTLM. If authentication still fails, the user is prompted to provide credentials. After authentication has taken place, the data stream is encrypted as a function of either the Kerberos protocol or SSL, if NTLM is used.

In the case of a Reporting Server and a management server, after authentication has occurred, a data connection is established between the management server and SQL Server Reporting Server. This is accomplished by strictly using the Kerberos protocol; therefore, the management server and Reporting Server must reside in trusted domains. For more information about WCF, see the MSDN article [What Is Windows Communication Foundation](#).

Management Server and Reporting Data Warehouse

Two communication channels exist between a management server and the Reporting data warehouse:

- The monitoring host process spawned by the health service (System Center Management service) in a management server
- The System Center Data Access services in the management server

Monitoring Host Process and Reporting Data Warehouse

By default, the monitoring host process spawned by the Health Service, which is responsible for writing collected events and performance counters to the data warehouse, achieves Windows Integrated Authentication by running as the Data Writer Account specified during Reporting Setup. The account credential is securely stored in a Run As Account called Data Warehouse Action Account. This Run As Account is a member of a Run As Profile called Data Warehouse Account (which is associated with the actual collection rules).

If the Reporting data warehouse and the management server are separated by a trust boundary (for example, each resides in different domains with no trust), then Windows Integrated Authentication will not work. To work around this situation, the monitoring host process can connect to the Reporting data warehouse using SQL Server Authentication. To do this, create a new Run As Account (of Simple Account type) with the SQL account credential and make it a member of the Run As Profile called Data Warehouse SQL Server Authentication Account, with the management server as the target computer.

Important

By default, the Run As Profile, Data Warehouse SQL Server Authentication Account was assigned a special account through the use of the Run As Account of the same name. Never make any changes to the account that is associated with the Run As Profile, Data Warehouse SQL Server Authentication Account. Instead, create your own account and your own Run As Account and make the Run As Account a member of the Run As Profile, Data Warehouse SQL Server Authentication Account when configuring SQL Server Authentication.

The following outlines the relationship of the various account credentials, Run As Accounts, and Run As Profiles for both Windows Integrated Authentication and SQL Server Authentication.

Default: Windows Integrated Authentication

Run As Profile: Data Warehouse Account

Run As Account: Data Warehouse Action Account

Credentials: Data Writer Account (specified during setup)

Run As Profile: Data Warehouse SQL Server Authentication Account

Run As Account: Data Warehouse SQL Server Authentication Account

Credentials: Special account created by Operations Manager (do not change)

Optional: SQL Server Authentication

Run As Profile: Data Warehouse SQL Server Authentication Account

Run As Account: A Run As Account you create.

Credentials: An account you create.

The System Center Data Access Service and Reporting Data Warehouse

By default, the System Center Data Access service, which is responsible for reading data from the Reporting data warehouse and making it available in the Report Parameter Area, achieves Windows Integrated Authentication by running as the Data Access Service and Config Service account that was defined during setup of Operations Manager.

If the Reporting data warehouse and the management server are separated by a trust boundary (for example, each resides in different domains with no trust), then Windows Integrated Authentication would not work. To work around this situation, the System Center Data Access service can connect to the Reporting data warehouse using SQL Server Authentication. To do this, create a new Run As Account (of Simple Account type) with the SQL account credential and make it a member of the Run As Profile called Reporting SDK SQL Server Authentication Account with the management server as the target computer.

Important

By default, the Run As Profile, Reporting SDK SQL Server Authentication Account was assigned a special account through the use of the Run As Account of the same name. Never make any changes to the account that is associated with the Run As Profile, Reporting SDK SQL Server Authentication Account. Instead, create your own account and your own Run As Account, and make the Run As Account a member of the Run As Profile, Reporting SDK SQL Server Authentication Account when configuring SQL Server Authentication.

The following outlines the relationship of the various account credentials, Run As Accounts, and Run As Profiles for both Windows Integrated Authentication and SQL Server Authentication.

Default: Windows Integrated Authentication

Data Access Service and Config Service Account (defined during setup of Operations Manager)

Run As Profile: Reporting SDK SQL Server Authentication Account

Run As Account: Reporting SDK SQL Server Authentication Account

Credentials: Special account created by Operations Manager (do not change)

Optional: SQL Server Authentication

Run As Profile: Data Warehouse SQL Server Authentication Account

Run As Account: A Run As Account you create.

Credentials: An account you create.

Operations Console and Reporting Server

The Operations console connects to Reporting Server on port 80 using HTTP. Authentication is performed by using Windows Authentication. Data can be encrypted by using the SSL channel. For more information about using SSL between the Operations console and Reporting Server, see [How to Configure the Operations Console to Use SSL When Connecting to a Reporting Server](#).

Reporting Server and Reporting Data Warehouse

Authentication between Reporting Server and the Reporting data warehouse is accomplished using Windows Authentication. The account that was specified as the Data Reader Account during setup of Reporting becomes the Execution Account on Reporting Server. If the password for the account should change, you will need to make the same password change using the Reporting Services Configuration Manager in SQL Server. For more information about resetting this password, see [How to Change the Reporting Server Execution Account Password](#). The data between the Reporting Server and the Reporting data warehouse is not encrypted.

How to Obtain a Certificate Using Windows Server 2008 Enterprise CA

Use the procedures in this topic to obtain a certificate from Windows Server 2008 R2, or Windows Server 2008 R2 SP1 computer hosting Enterprise Root Active Directory Certificate Services (AD CS). You use the CertReq command-line utility to request and accept a certificate, and you use a Web interface to submit and retrieve your certificate.

It is assumed that you have AD CS installed, an HTTPS binding has been created, and its associated certificate has been installed. Information about creating an HTTPS binding is available in the topic [How to Configure an HTTPS Binding for a Windows Server 2008 CA](#).

Important

The content for this topic is based on the default settings for Windows Server 2008 AD CS; for example, setting the key length to 2048, selecting Microsoft Software Key Storage Provider as the CSP, and using Secure Hash Algorithm 1 (SHA1). Evaluate these selections against the requirements of your company's security policy.

The high-level process to obtain a certificate from an Enterprise certification authority (CA) is as follows:

1. [Download the Trusted Root \(CA\) certificate](#).
2. [Import the Trusted Root \(CA\) certificate](#).
3. [Create a certificate template](#).
4. [Add the template to the Certificate Templates folder](#).
5. [Create a setup information file for use with the CertReq command-line utility](#).
6. [Create a request file](#).
7. [Submit a request to the CA](#).

8. [Import the certificate into the certificate store.](#)
9. [Import the certificate into Operations Manager using MOMCertImport.](#)

Download the Trusted Root (CA) certificate

▶ To download the Trusted Root (CA) certificate

1. Log on to the computer where you want to install a certificate; for example, the gateway server or management server.
2. Start Internet Explorer, and connect to the computer hosting Certificate Services; for example, <https://<servername>/certsrv>.
3. On the **Welcome** page, click **Download a CA Certificate, certificate chain, or CRL**.
4. On the **Download a CA Certificate, Certificate Chain, or CRL** page, click **Encoding method**, click **Base 64**, and then click **Download CA certificate chain**.
5. In the **File Download** dialog box, click **Save** and save the certificate; for example, **Trustedca.p7b**.
6. When the download has finished, close Internet Explorer.

Import the Trusted Root (CA) certificate

▶ To import the Trusted Root (CA) Certificate

1. On the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **mmc**, and then click **OK**.
3. In the **Console1** window, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
6. In the **Certificates snap-in** dialog box, select **Computer account**, and then click **Next**.
7. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.
10. In the **Console1** window, expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
11. Right-click **Certificates**, select **All Tasks**, and then click **Import**.
12. In the Certificate Import Wizard, click **Next**.
13. On the **File to Import** page, click **Browse** and select the location where you downloaded the CA certificate file, for example, **TrustedCA.p7b**, select the file, and then click **Open**.
14. On the **File to Import** page, select **Place all certificates in the following store** and ensure that **Trusted Root Certification Authorities** appears in the **Certificate store** box, and then click **Next**.
15. On the **Completing the Certificate Import Wizard** page, click **Finish**.

Create a certificate template

▶ **To create a certificate template**

1. On the computer that is hosting your enterprise CA, on the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**.
2. In the navigation pane, expand the CA name, right-click **Certificate Templates**, and then click **Manage**.
3. In the **Certificate Templates** console, in the results pane, right-click **IPsec (Offline request)**, and then click **Duplicate Template**.
4. In the **Duplicate Template** dialog box, select **Windows Server 2008 Enterprise Edition**, and then click **OK**.
5. In the **Properties of New Template** dialog box, on the **General** tab, in the **Template display name** text box, type a new name for this template; for example, **OperationsManagerCert**.
6. On the **Request Handling** tab, select **Allow private key to be exported**.
7. Click the **Extensions** tab, and in **Extensions included in this template**, click **Application Policies**, and then click **Edit**.
8. In the **Edit Application Policies Extension** dialog box, click **IP security IKE intermediate**, and then click **Remove**.
9. Click **Add**, and in the **Application policies list**, hold down the CTRL key to multi-select items from the list, click **Client Authentication** and **Server Authentication**, and then click **OK**.
10. In the **Edit Application Policies Extension** dialog box, click **OK**.
11. Click the **Security** tab and ensure that the **Authenticated Users** group has **Read** and **Enroll** permissions, and then click **OK**.
12. Close the Certificate Templates console.

Add the template to the Certificate Templates folder

▶ **To add the template to the Certificate Templates folder**

1. On the computer that is hosting your Enterprise CA, in the Certification Authority snap-in, right-click the **Certificate Templates** folder, point to **New**, and then click **Certification Template to Issue**.
2. In the **Enable Certificate Templates** box, select the certificate template that you created; for example, click **OperationsManagerCert**, and then click **OK**.

Create a setup information file for use with the CertReq command-line utility

▶ **To create a setup information (.inf) file**

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **Notepad**, and then click **OK**.

3. Create a text file containing the following content:
[NewRequest]
Subject="CN=<FQDN of computer you are creating the certificate, for example, the gateway server or management server.>"
Exportable=TRUE
KeyLength=2048
KeySpec=1
KeyUsage=0xf0
MachineKeySet=TRUE
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
OID=1.3.6.1.5.5.7.3.2
4. Save the file with an .inf file name extension; for example, RequestConfig.inf.
5. Close Notepad.

Create a request file

▶ To create a request file to use with an enterprise CA

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. In the command window, type **CertReq -New -f RequestConfig.inf CertRequest.req**, and then press ENTER.
4. Using Notepad, open the resulting file (for example, CertRequest.req), and copy the contents of this file into the clipboard.

Submit a request to the CA

▶ To submit a request to an enterprise CA

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, start Internet Explorer, and then connect to the computer hosting Certificate Services; for example, <https://<servername>/certsrv>.



Note

If an HTTPS binding has not been configured on the Certificate Services Web site, the browser will fail to connect. See the topic **How to Configure an HTTPS Binding for a Windows Server 2008 CA** in this guide.

2. On the **Microsoft Active Directory Certificate Services Welcome** screen, click **Request a certificate**.
3. On the **Request a Certificate** page, click **advanced certificate request**.
4. On the **Advanced Certificate Request** page, click **Submit a certificate request by**

using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

5. On the **Submit a Certificate Request or Renewal Request** page, in the **Saved Request** text box, paste the contents of the CertRequest.req file that you copied in step 4 in the previous procedure.
6. In the **Certificate Template** select the certificate template that you created, for example, OperationsManagerCert, and then click **Submit**.
7. On the **Certificate Issued** page, select **Base 64 encoded**, and then click **Download certificate**.
8. In the **File Download – Security Warning** dialog box, click **Save**, and save the certificate; for example, save as NewCertificate.cer.
9. Close Internet Explorer.

Import the certificate into the certificate store

▶ To import the certificate into the certificate store

1. On the computer hosting the Operations Manager feature for which you are configuring the certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. In the command window, type **CertReq –Accept NewCertificate.cer**, and then press ENTER.

Import the certificate into Operations Manager using MOMCertImport

▶ To import the certificate into Operations Manager using MOMCertImport

1. Log on to the computer where you installed the certificate with an account that is a member of the Administrators group.
2. On the Windows desktop, click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **cmd**, and then click **OK**.
4. At the command prompt, type **<drive_letter>:** (where *<drive_letter>* is the drive where the Operations Manager installation media is located), and then press ENTER.
5. Type **cd\SupportTools\i386**, and then press ENTER.



Note

On 64-bit computers, type **cd\SupportTools\amd64**

6. Type the following:
MOMCertImport /SubjectName <Certificate Subject Name>
7. Press ENTER.

See Also

[Authentication and Data Encryption for Windows Computers](#)

How to Obtain a Certificate Using Windows Server 2008 Stand-Alone CA

Use the procedures in this topic to obtain a certificate from a stand-alone Windows Server 2008 R2, or Windows Server 2008 R2 SP1–based computer hosting Active Directory Certificate Services (AD CS). You use the CertReq command-line utility to request and accept a certificate, and you use a Web interface to submit and retrieve your certificate.

It is assumed that you have AD CS installed, an HTTPS binding is being used, and its associated certificate has been installed. Information about creating an HTTPS binding is available in the topic [How to Configure an HTTPS Binding for a Windows Server 2008 CA](#).

Important

The content for this topic is based on the default settings for Windows Server 2008 AD CS; for example, setting the key length to 2048, selecting Microsoft Software Key Storage Provider as the CSP, and using Secure Hash Algorithm 1 (SHA1). Evaluate these selections against the requirements of your company's security policy.

The high-level process to obtain a certificate from a stand-alone certification authority (CA) is as follows:

1. [Download the Trusted Root \(CA\) certificate](#).
2. [Import the Trusted Root \(CA\) certificate](#)
3. [Create a setup information file](#) to use with the CertReq command-line utility.
4. [Create a request file](#).
5. [Submit a request to the CA using the request file](#).
6. [Approve the pending certificate request](#).
7. [Retrieve the certificate from the CA](#).
8. [Import the certificate into the certificate store](#).
9. [Import the certificate into Operations Manager using MOMCertImport](#).

Download the Trusted Root (CA) certificate

To download the Trusted Root (CA) certificate

1. Log on to the computer where you want to install a certificate; for example, the gateway server or management server.
2. Start Internet Explorer, and connect to the computer hosting Certificate Services; for example, <https://<servername>/certsrv>.
3. On the **Welcome** page, click **Download a CA Certificate, certificate chain, or CRL**.
4. On the **Download a CA Certificate, Certificate Chain, or CRL** page, click **Encoding method**, click **Base 64**, and then click **Download CA certificate chain**.
5. In the **File Download** dialog box, click **Save** and save the certificate; for example, **Trustedca.p7b**.
6. When the download has finished, close Internet Explorer.

Import the Trusted Root (CA) certificate

To import the Trusted Root (CA) Certificate

1. On the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **mmc**, and then click **OK**.
3. In the **Console1** window, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
6. In the **Certificates snap-in** dialog box, select **Computer account**, and then click **Next**.
7. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.
10. In the **Console1** window, expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
11. Right-click **Certificates**, select **All Tasks**, and then click **Import**.
12. In the Certificate Import Wizard, click **Next**.
13. On the **File to Import** page, click **Browse** and select the location where you downloaded the CA certificate file, for example, TrustedCA.p7b, select the file, and then click **Open**.
14. On the **File to Import** page, select **Place all certificates in the following store** and ensure that **Trusted Root Certification Authorities** appears in the **Certificate store** box, and then click **Next**.
15. On the **Completing the Certificate Import Wizard** page, click **Finish**.

Create a setup information file

► To create a setup information (.inf) file

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **Notepad**, and then click **OK**.
3. Create a text file containing the following content:

[NewRequest]

Subject="CN=<FQDN of computer you are creating the certificate, for example, the gateway server or management server.>"

Exportable=TRUE

KeyLength=2048

KeySpec=1

KeyUsage=0xf0

MachineKeySet=TRUE

[EnhancedKeyUsageExtension]

OID=1.3.6.1.5.5.7.3.1

OID=1.3.6.1.5.5.7.3.2

4. Save the file with an .inf file name extension, for example, RequestConfig.inf.
5. Close Notepad.

Create a request file

▶ To create a request file to use with a stand-alone CA

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. In the command window, type **CertReq -New -f RequestConfig.inf CertRequest.req**, and then press ENTER.
4. Open the resulting file (for example, CertRequest.req) with Notepad. Copy the contents of this file onto the clipboard.

Submit a request to the CA using the request file

▶ To submit a request to a stand-alone CA

1. On the computer hosting the Operations Manager feature for which you are requesting a certificate, start Internet Explorer, and then connect to the computer hosting Certificate Services (for example, https://<servername>/certsrv).



Note

If an HTTPS binding has not been configured on the Certificate Services Web site, the browser will fail to connect. For more information, see [How to Configure an HTTPS Binding for a Windows Server 2008 CA](#).

2. On the **Microsoft Active Directory Certificate Services Welcome** screen, click **Request a certificate**.
3. On the **Request a Certificate** page, click **advanced certificate request**.
4. On the **Advanced Certificate Request** page, click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.
5. On the **Submit a Certificate Request or Renewal Request** page, in the **Saved Request** text box, paste the contents of the CertRequest.req file that you copied in step 4 in the previous procedure, and then click **Submit**.
6. Close Internet Explorer.

Approve the pending certificate request

▶ To approve the pending certificate request

1. Log on as a certification authority administrator to the computer hosting Active Directory Certificate Services.
2. On the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**.

3. In **Certification Authority**, expand the node for your certification authority name, and then click **Pending Requests**.
4. In the results pane, right-click the pending request from the previous procedure, point to **All Tasks**, and then click **Issue**.
5. Click **Issued Certificates**, and confirm the certificate you just issued is listed.
6. Close Certification Authority.

Retrieve the certificate from the CA

▶ To retrieve the certificate

1. Log on to the computer where you want to install a certificate; for example, the gateway server or management server.
2. Start Internet Explorer, and connect to the computer hosting Certificate Services (for example, <https://<servername>/certsrv>).
3. On the **Microsoft Active Directory Certificate Services Welcome** page, click **View the status of a pending certificate request**.
4. On the **View the Status of a Pending Certificate Request** page, click the certificate you requested.
5. On the **Certificate Issued** page, select **Base 64 encoded**, and then click **Download certificate**.
6. In the **File Download – Security Warning** dialog box, click **Save**, and save the certificate; for example, as **NewCertificate.cer**.
7. On the **Certificate Installed** page, after you see the message that **Your new certificate has been successfully installed**, close the browser.
8. Close Internet Explorer.

Import the certificate into the certificate store

▶ To import the certificate into the certificate store

1. On the computer hosting the Operations Manager feature for which you are configuring the certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. In the command window, type **CertReq –Accept NewCertificate.cer**, and then press ENTER.

Import the certificate into Operations Manager using MOMCertImport

▶ To import the certificate into Operations Manager using MOMCertImport

1. Log on to the computer where you installed the certificate with an account that is a member of the Administrators group.
2. On the Windows desktop, click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **cmd**, and then click **OK**.

4. At the command prompt, type `<drive_letter>:` (where `<drive_letter>` is the drive where the Operations Manager installation media is located), and then press ENTER.
5. Type `cd\SupportTools\i386`, and then press ENTER.



Note

On 64-bit computers, type `cd\SupportTools\amd64`

6. Type the following:
MOMCertImport /SubjectName <Certificate Subject Name>
7. Press ENTER.

See Also

[Authentication and Data Encryption for Windows Computers](#)

How to Configure an HTTPS Binding for a Windows Server 2008 CA

If you are setting up a new certification authority (CA) for the first time for use with System Center 2012 – Operations Manager, use the following procedure to configure an HTTPS binding for the CA.

► To configure an HTTPS binding

1. On the computer hosting your CA, on the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the **Internet Information Services (IIS) Manager** dialog box, in the **Connections** pane, expand your computer name, expand **Sites**, and then click **Default Web Site**.
3. In the **Actions** pane, click **Bindings**.
4. In the **Site Bindings** dialog box, click **Add**.
5. In the **Add Site Binding** dialog box, on the **Type** menu, select **https**.
6. In the **SSL Certificate** list, select the entry that matches the name of your computer, and then click **OK**.
7. In the **Site Bindings** dialog box, click **Close**.
8. In the **Connections** pane, under **Default Web Site**, click **CertSrv**.
9. In the **/CertSrv Home** pane, right-click **SSL Settings**, and then click **Open Feature**.
10. In the **SSL Settings** pane, click **Require SSL**.
11. In the **Actions** pane, click **Apply**, and then close Internet Information Services (IIS) Manager.

Deploying ACS and ACS Reporting

In System Center 2012 – Operations Manager, Audit Collection Services (ACS) provides a means to collect records generated by an audit policy and store them in a centralized database. Using ACS, organizations can consolidate individual Security logs into a centrally managed database and can filter and analyze events using the data analysis and reporting tools provided

by Microsoft SQL Server. For more information, see [Collecting Security Events Using Audit Collection Services in Operations Manager 2012](#)

Audit Collection Services (ACS) reporting can be installed in two configurations.

- A supported version of Microsoft SQL Server Reporting Services (SSRS) instance with Operations Manager Reporting already installed. A benefit of this is the ability to view ACS Reports in the Operations console.
- An SSRS instance without Operations Manager Reporting installed.

The installation procedures for ACS Reporting do not differ, but the application of access control is different. By deploying ACS Reporting on the same SQL Server Reporting Services instance as your Operations Manager Reporting, the same role-based security applies to all reports. This means that ACS Reporting users need to be assigned to the Operations Manager Report Operator Role to access the ACS reports.

In addition to membership in the Operations Manager Reporting Role, ACS report users must also be assigned db_datareader role on the ACS database (OperationsManagerAC) to run ACS reports. This requirement is independent of the presence of Operations Manager Reporting

If you choose to install ACS Reporting independently of Operations Manager Reporting, you can also use SSRS security to secure the reports. For more information, see the SQL Server Books Online tutorial [Tutorial: Setting Permissions in Reporting Services](#).

Preparing for installation

Deploy ACS as described in the following topics prior to installing ACS Reporting.

- [How to Install Audit Collection Services \(ACS\)](#)
- [How to Deploy ACS on a Secondary Management Server](#)
- [How to Install an Audit Collection Services \(ACS\) Collector and Database](#)
- [How to Deploy Audit Collection Services for UNIX/Linux](#)

► Before you start

1. A management server for your management group must be installed and ACS must be configured on the management server. For more information, see [Collecting Security Events Using Audit Collection Services in Operations Manager](#).
2. An instance of a supported version of Microsoft SQL Server Reporting Services must be installed on the target computer.
3. During the procedure, you need to be logged on as member of Operations Manager Report Operator user role.
4. IIS must be installed on the hosting system. IIS will have already been installed if you are co-locating with a Reporting server.
5. You need to have access to the ACS database.
6. You need the Operations Manager installation media.

The following content will help you install ACS on a secondary management server, and install ACS Reporting.

- [How to Deploy ACS on a Secondary Management Server](#)
- [How to Deploy ACS Reporting](#)

How to Install Audit Collection Services (ACS)

The following procedure provides the general steps needed to install the System Center 2012 – Operations Manager Audit Collection Services (ACS) feature within your organization.



Note

To uninstall Operations Manager from the management server that functions as your ACS Collector, you must first uninstall ACS.

See [Collecting Security Events Using Audit Collection Services in Operations Manager](#) in the Operations Guide for information on minimum and recommended system requirements for ACS.

► To install Audit Collection Services

1. Plan an audit policy for your organization. For more information on setting up an audit policy, see [Advanced Security Audit Policy Step-by-Step Guide](#).
2. Plan your ACS server deployment. This includes deciding which server will act as the ACS database and which management server will act as the ACS collector. Ensure that the computers selected for these roles meet the minimum system requirements. See [Collecting Security Events Using Audit Collection Services in Operations Manager](#) in the Operations Guide for more information about ACS and the system requirements for each feature.
3. Plan which Operations Manager agents will be ACS forwarders. All computers that you want to collect security events from must be ACS forwarders.
4. Install and configure prerequisites for ACS features.
5. (Optional) Separate administrator and auditor roles by doing the following:
 - a. Create a local group just for users who access and run reports on the data in the ACS database. For step-by-step instructions for creating a local group, see the “To create a group account in Active Directory” section of the “Creating user and group accounts” topic at <http://go.microsoft.com/fwlink/?LinkId=74159>.
 - b. Grant the newly created local group access to the SQL database by creating a new SQL Login for the group and assigning that login the db_datareader permission. For step-by-step instructions for creating a SQL Login, go to [Set up a user account on a SQL server](#).
 - c. Add the user accounts of users who will act as auditors to the local group.
6. Deploy the ACS Database and ACS Collector(s). See [How to Install an Audit Collection Services \(ACS\) Collector and Database](#).
7. Run the **Enable Audit Collection** task to start the ACS Forwarder service on the ACS forwarders. For more information, see [How to Enable Audit Collection Services \(ACS\) Forwarders](#).
8. Implement your audit policy within your organization.

See Also

[Deploying ACS and ACS Reporting](#)

[How to Install an Audit Collection Services \(ACS\) Collector and Database](#)

[How to Deploy ACS on a Secondary Management Server](#)

[How to Deploy ACS Reporting](#)

How to Install an Audit Collection Services (ACS) Collector and Database

Use the following procedures in System Center 2012 – Operations Manager to install an Audit Collection Services (ACS) collector and database and to start the service for the ACS collector computer. Both procedures are performed on the computer that is designated as your ACS collector.

The ACS database runs on a supported version of Microsoft SQL Server. The Audit Collection Services Collector Setup wizard creates the ACS database on an existing installation of Microsoft SQL Server. To complete the installation procedure, you must be a member of the local Administrators group on both the ACS collector and the ACS database computers as well as a database administrator on the ACS database. As a best practice for security, consider using Run As to perform this procedure.

For information about system requirements and best practices for performance, see [Collecting Security Events Using Audit Collection Services in Operations Manager](#) and [Audit Collection Services Capacity Planning](#) in the Operations Guide.

► To install an ACS collector and an ACS database

1. Log on to the server by using an account that has local administrative credentials.
2. On the Operations Manager installation media, run **Setup.exe**, and then click **Audit collection services**.

For monitoring UNIX and Linux computers, click **Audit collection services for UNIX/Linux**.

The **Audit Collection Services Collector Setup** wizard opens.

3. On the **Welcome** page, click **Next**.
4. On the **License Agreement** page, read the licensing terms, click **I accept the agreement**, and then click **Next**.
5. On the **Database Installation Options** page, click **Create a new database**, and then click **Next**.
6. On the **Data Source** page, in the **Data source name** box, type a name that you want to use as the Open Database Connectivity (ODBC) data source name for your ACS database. By default, this name is **OpsMgrAC**. Click **Next**.
7. On the **Database** page, if the database is on a separate server than the ACS collector, click **Remote Database Server**, and then type the computer name of the database server that will host the database for this installation of ACS. Otherwise, click **Database server running locally**.
8. In the **Database server instance name** field, type the name of the database that will be created for ACS. If you leave this field blank, the default name is used. In the **Database**

name field, the default database name of **OperationsManagerAC** is automatically entered. You can select the text and type in a different name or leave the default name. Click **Next**.



Note

To display a list of SQL Server Instances, on the database computer click **Start**, point to **Programs** and open **SQL Server** (the appropriate version of SQL Server is dependent on the version of Operations Manager – see [System Requirements for System Center 2012 – Operations Manager](#)), and then click **SQL Server Management Studio**. On the **Server name** list, click **Browse for more** and then expand **Database Engine**. All databases are listed as server name\database name.

9. On the **Database Authentication** page, select one of the authentication methods. If the ACS collector and the ACS database are members of the same domain, you can select **Windows authentication**, otherwise select **SQL authentication**, and then click **Next**.



Note

If you select **SQL authentication** and click **Next**, the **Database Credentials** page displays. In the **SQL login name** box, enter the name of the user account that has access to the SQL Server and the password for that account in the **SQL password** box, and then click **Next**.

10. On the **Database Creation Options** page, click **Use SQL Server's default data and log file directories** to use SQL Server's default folders. Otherwise, click **Specify directories** and enter the full path, including drive letter, to the location you want for the ACS database and log file, for example C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data. Click **Next**.
11. On the **Event Retention Schedule** page, click **Local hour of day to perform daily database maintenance**. Choose a time when the number of expected security events is low. During the database maintenance period, database performance will be impacted. In the **Number of days to retain events** box type the number of days ACS should keep events in the ACS database before the events are removed during database grooming. The default value is 14 days. Click **Next**.
12. On the **ACS Stored Timestamp Format** page, choose **Local** or **Universal Coordinated Time**, formerly known to as Greenwich Mean Time, and then click **Next**
13. The **Summary** page displays a list of actions that the installation program will perform to install ACS. Review the list, and then click **Next** to begin the installation.



Note

If a **SQL server login** dialog box displays and the database authentication is set to **Windows authentication**, click the correct database and verify that the **Use Trusted Connection** check box is checked. Otherwise click to remove the check and enter the SQL login name and password. Click **OK**.

14. When the installation is complete, click **Finish**.

See Also

[Deploying ACS and ACS Reporting](#)

[How to Install Audit Collection Services \(ACS\)](#)

[How to Deploy ACS on a Secondary Management Server](#)

[How to Deploy ACS Reporting](#)

How to Deploy ACS on a Secondary Management Server

In this procedure, the Audit Collection Services Collector and the Audit Collection Services (ACS) databases are installed on different servers, with the ACS Collector on a stand-alone management server and the ACS database on a separate database. The Operations Manager ACS Collector service must be installed on an existing management server. You can also choose to create a database for ACS to use or you can let the setup program create one for you. In this procedure, an already existing stand-alone secondary management server is used for the ACS Collector and a new ACS Database is created by the ACS setup. For an overview of ACS, see [Collecting Security Events Using Audit Collection Services in Operations Manager 2012](#).

When you are done with this procedure, you must enable the ACS forwarder function on all Operations Manager Agents that you want to collect Windows Security Event Log events from. For more information about enabling ACS forwarders, see [How to Enable ACS Forwarders](#).

► To install ACS on a secondary management server

1. Log on to the secondary management server that is to host the ACS Collector with the domain-based Operations Manager Administrator account. This account should already have local administrative rights.
2. On the Operations Manager installation media, start **Setup.exe**.
3. Under the **Install** heading, click the **Audit collection services** link. The **Audit Collection Services Collector Setup** wizard opens.
4. On the **Welcome** page, click **Next**.
5. On the **License Agreement** page, select the **I accept the agreement** option and click **Next**.
6. On the **Database Installation Options** page, select the **Create a new database** option. This creates the ACS database on the designated instance of SQL Server with the necessary tables and stored procedures and the SQL login and database user for the collector. Click **Next**.
7. On the **Data Source** page, in the **Data Source name** field, accept the default value of **OpsMgrAC**, and then click **Next**.



Note

The ACS Collector uses an Open Database Connectivity (ODBC) Data Source Name (DSN) to communicate with the ACS database.

8. On the **Database** page, select the **Remote database server** option. In the **Remote database server machine name** field, enter the value in the name field of the SQL Server network. Leave the **Database server instance name** field blank, unless you have installed a SQL Server cluster in a named instance of SQL Server, and then enter that

- value. In the **Database name** field, accept the default of **OperationsManagerAC**, but if you plan to host multiple ACS databases in the same instance of SQL Server, enter a unique name. Click **Next**.
9. On the **Database Authentication** page, select **Windows authentication**, and then click **Next**. By selecting Windows authentication, the ACS Collector services will use the local machine account to write to the ACS database during normal operations.
 10. On the **Database Creation Options** page, select the **Use SQL Server default data and log file directories** option, and then click **Next**.
 11. On the **Event Retention Schedule** page, set the **Local hour of day to perform daily maintenance** and **Number of days an event is retained in database** options to the appropriate values, and then click **Next**.
 12. On the **ACS Stored Timestamp Format** page, select either the **Local** or **Universal Coordinated Time (UTC)** option, and then click **Next**.
 13. On the **Summary** page, review the installation options, and then click **Next**.
 14. During the installation, you might be prompted for a SQL Server Login. If you are logged on with an account that has SQL Server Administrator rights, then accept the default or otherwise provide credentials that have the SQL Server Administrator rights.

 **Note**

This account is used by the setup process to create the ACS database.

15. Click **Finish** to complete the installation.
16. Open the **SQL Server Management Studio** tool, open the **Databases** folder, and confirm the presence of the **OperationsManagerAC** database.
17. On the ACS management server, open **Server Manager** tool, expand the **Configuration** container and select **Services**, and confirm that the **Operations Manager Audit Collection Service** is present, that it is started, and that the **Startup Type** is set to **Automatic**.
18. You can now enable the ACS forwarders. For more information, see [How to Enable ACS Forwarders](#).

See Also

[Deploying ACS and ACS Reporting](#)

[How to Install an Audit Collection Services \(ACS\) Collector and Database](#)

[How to Install Audit Collection Services \(ACS\)](#)

[How to Deploy ACS Reporting](#)

How to Deploy ACS Reporting

You deploy Audit Collection Services (ACS) Reporting on a supported version of Microsoft SQL Server Reporting Services (SSRS) instance. If System Center 2012 – Operations Manager Reporting has also been installed on the same SSRS instance, you can view the ACS Reports in the Operations console. Before you deploy ACS, there are a number of prerequisite steps you must perform, such as ensuring that a ACS is configured on management server within your management group. For more information, see [Deploying ACS and ACS Reporting](#).

► To deploy ACS Reporting

1. Log on to the server that will be used to host ACS reporting as a user that is an administrator of the SSRS instance.
2. Create a temporary folder, such as **C:\acs**.
3. On your installation media, go to **\ReportModels\acs** and copy the directory contents to the temporary installation folder.

There are two folders (**Models** and **Reports**) and a file named **UploadAuditReports.cmd**.

4. On your installation media, go to **\SupportTools** and copy the file **ReportingConfig.exe** into the temporary **acs** folder.
5. Open a Command Prompt window by using the **Run as Administrator** option, and then change directories to the temporary **acs** folder.
6. Run the following command.

```
UploadAuditReports "<AuditDBServer\Instance>" "<Reporting Server URL>"  
"<path of the copied acs folder>"
```

For example: **UploadAuditReports "myAuditDbServer\Instance1"
"http://myReportServer/ReportServer\$instance1" "C:\acs"**

This example creates a new data source called **Db Audit**, uploads the reporting models **Audit.smdl** and **Audit5.smdl**, and uploads all reports in the **acs\reports** directory.



Note

The reporting server URL needs the reporting server virtual directory (**ReportingServer_<InstanceName>**) instead of the reporting manager directory (**Reports_<InstanceName>**).

7. Open Internet Explorer and enter the following address to view the **SQL Reporting Services Home** page. **http://<yourReportingServerName>/Reports_<InstanceName>**
8. Click **Audit Reports** in the body of the page and then click **Show Details** in the upper right part of the page.
9. Click the **Db Audit** data source.
10. In the **Connect Using** section, select **Windows Integrated Security** and click **Apply**.

See Also

[Deploying ACS and ACS Reporting](#)

[How to Install an Audit Collection Services \(ACS\) Collector and Database](#)

[How to Deploy ACS on a Secondary Management Server](#)

[How to Install Audit Collection Services \(ACS\)](#)

How to Deploy Audit Collection Services for UNIX/Linux

This procedure describes the steps to deploy Audit Collection Services for UNIX/Linux to enable security event collection and reporting for monitored UNIX and Linux computers.

In this Topic

- [Prerequisite Configuration](#)
- [Installing Audit Collection Services for UNIX/Linux](#)
- [Importing UNIX and Linux ACS Management Packs](#)
- [Installing ACS Reports for UNIX/Linux](#)
- [How to Enable Audit Collection Services for UNIX/Linux](#)

Prerequisite Configuration

Before deploying Audit Collection Services for UNIX/Linux, ACS and ACS Reporting must be deployed and configured. See the following topic for information on deploying and configuring Audit Collection Services.

- [Deploying ACS and ACS Reporting](#)

Installing Audit Collection Services for UNIX/Linux

ACS for UNIX and Linux must be installed on each Management Server that manages UNIX or Linux computers. Complete this procedure for each required management server.

1. From a command prompt or the **Run** menu, launch **Services.msc**. Find the **System Center Audit Forwarding** service, and set the service start to **Automatic**. Start the service.
2. From the Operations Manager setup splash screen, select **Audit Collection Services for UNIX/Linux** from the **Optional Installations** section.
3. On the first page of the ACS for UNIX/Linux setup wizard, click **Next**.
4. Accept the terms of service, and then click **Next**.
5. Select **Audit Data Time Zone**, and then click **Next**.
6. On the Ready page, click **Install**.
7. On the ACS Audit Events page, click **Next**.
8. Click **Finish**.



Note

By default, events cannot be written directly to the Windows Security Event log. During installation, a local group policy is modified to allow the Cross Platform Audit Collection Services module to write to the Windows Security Event log.

The policy is found at **Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy -> Audit object access {Success, Failure}**. If group policy is overriding the local policy, it may be necessary to modify this group policy setting on the domain.

Importing UNIX and Linux ACS Management Packs

Audit Collection Services Management Packs for each required UNIX or Linux operating system must be imported for UNIX/Linux ACS event collection. To import UNIX and Linux ACS Management Packs, follow this procedure:

1. In the **Operations** console, click the **Administration** node.
2. Right-click **Management Packs**, and then click **Import Management Packs**.
3. In the Import Management Packs Wizard, select **Add**.
4. Select **Add from Disk**.

5. Browse to the **ManagementPacks** folder of the Operations Manager installation media.
6. Select ACS management packs appropriate for the UNIX-based and Linux-based computers you are monitoring. The ACS management packs have file names that begin with: **Microsoft.ACS**.
7. Select **Open**.
8. Select **Install** to start the import process.
9. When the import is complete, click **Close**.

Installing ACS Reports for UNIX/Linux

1. Log on to the server that will be used to host ACS reporting as a user that is an administrator of the SSRS instance.
2. Create a temporary folder, such as **C:\acs**.
3. From a server with Audit Collection Services for UNIX/Linux installed, copy the ACS reports to your temporary folder. The ACS reports can be found in the Program Files directory. For example: **C:\Program Files\System Center Operations Manager Cross Platform ACS\Cross Platform Audit Reports**.
4. Open a Command Prompt window by using the **Run as Administrator** option, and then change directories to the temporary **acs** folder.
5. Run the following command.

```
UploadCrossPlatformAuditReports "<AuditDBServer\Instance>"
"<Reporting Server URL>" "<path of the copied ACS folder>"
```

For example:

```
UploadCrossPlatformAuditReports "myAuditDbServer\Instance1"
"http://myReportServer/ReportServer$instance1" "C:\acs"
```

How to Enable Audit Collection Services for UNIX/Linux

After Audit Collection Services for UNIX/Linux has been installed, it must be enabled in order for events to be collected.

1. In the Operations Console, click **Authoring**.
2. Click **Object Discoveries**.
3. Search for **ACS**.
4. Right-click **Discover UNIX/Linux ACS Endpoint**.
5. Select **Overrides -> Override the Object Discovery -> For all objects of class -> UNIX/Linux Computer**.



Note

As an alternative to enabling for all UNIX/Linux Computers, you can select individual computers and groups.

6. Select the **Enabled** check box.
7. In the Enabled Value list, select **True**.
8. In the **Management Pack** list, verify that the custom override management pack you created is selected.

9. Click **OK**.

See Also

[Deploying ACS and ACS Reporting](#)

Collecting Security Events Using Audit Collection Services in Operations Manager

Using SQL Server 2012 Always On Availability Groups with System Center 2012 SP1 - Operations Manager

System Center 2012 Service Pack 1 (SP1), Operations Manager supports SQL Server 2012 AlwaysOn functionality.

The procedures explained here are not intended to provide detailed instructions on how to configure a SQL 2012 AlwaysOn Availability Group, but instead provide tasks that need to be exercised in order for Operations Manager to work effectively when using availability groups, and also emphasizes specific SQL Server AlwaysOn functionality that SP1 supports.

For more information on SQL Server 2012 AlwaysOn Availability Groups, see [AlwaysOn Availability Groups \(SQL Server\)](#). A Word document describing SQL Server 2012 AlwaysOn Multisite Failover Cluster Instances can be found at [SQL Server 2012 AlwaysOn: Multisite Failover Cluster Instance](#).

 **Important**

We do not support a topology where the reporting FCI (the instance hosting the reporting services database only) is configured as part of the AlwaysOn Availability Group.

 **Note**

Operations Manager does not support setting the MultiSubnetFailover parameter. This parameter is not used in Operations Manager connection strings.

SQL 2012 AlwaysOn supported Operations Manager databases

 **SQL 2012 AlwaysOn supports the following Operations Manager databases.**

- Operations Manager Operational database
- Operations Manager Data Warehouse
- Operations Manager Audit Collection Services (ACS) database

 **Important**

For the Operations Manager Data Warehouse and the Operations Manager Audit Collection Services (ACS) database, see the procedures in [How to Move the Data Warehouse Database](#), but replace the new SQL server in the procedure with the <name,port> of the Availability group listener.

 **Note**

A common deployment pattern prescribes using separate SQL Server instances for the Operations Manager, Operations Manager Data Warehouse, and Operations Manager ACS databases. If you are using this pattern, then ensure that all SQL Server instances are added to the availability group.

New Management Group Installation

Use the following series of tasks when installing a new management group with a SQL 2012 AlwaysOn Availability Group.

▶ Before Installing Operations Manager on an availability group

1. Make sure to use the Group listener Name and port when installing Operations Manager for the databases that are going to be added to the availability databases.
2. The first management server will use the Group listener to get the primary SQL instance, and will install the databases on that instance.

▶ After installing the first management server

1. Ensure that the recovery model of the database is full: open SQL Server Management Studio and connect to the instance where the database(s) are installed. Right click on the targeted database, and select its **properties** and select **Options**. If the recovery model is not listed as “Full”, select **Full** from the drop down list.
2. Make a full back up the databases.
3. Use SQL Server Management Studio to add the databases to the availability databases. Notice that when adding the databases to the availability databases under **Select Data Synchronization**, three choice are possible: **Full**, **Join only** and **Skip initial data synchronization**. Choose the option that is most appropriate for you. We recommend selecting **Full** and allowing the **Add Database wizard** create a full backup and restore of the databases on the secondary replicas. More steps might or might not be needed depending on which choice you made. See [Manually Prepare a Secondary Database for an Availability Group \(SQL Server\)](#) for more information.
4. On the new server hosting the operational database, expand **Security**, then expand **Logins**, and add the data writer account name. For more information on how to create a SQL Server login, see [Create a Login](#).
5. Under **Logins**, add the action account.
6. Under **Logins**, add the Data Access Service (DAS) computer account, using the form “**domain\computername\$**”.
7. For the DAS computer account, add the following user mappings:
 - a. ConfigService
 - b. db_accessadmin
 - c. db_datareader
 - d. db_datawriter
 - e. db_ddladmin
 - f. db_securityadmin

- g. sdk_users
 - h. sql_dependency_subscriber
8. On the new server hosting the data warehouse database, expand **Security**, then expand **Logins**, and then add the data writer account. For more information on how to create a SQL Server login, see [Create a Login](#).
 9. Under **Logins**, add the data reader account.
 10. Under **Logins**, add the Data Access Service computer account, using the form “domain\computername\$”.
 11. For the DAS computer account, add the following user mappings:
 - a. db_datareader
 - b. OpsMgrReader
 - c. apm_datareader

Known Issues

When you open the Operations Manager console after failing from one node to the other you might encounter the following issue:

Execution of user code in the .NET Framework is disabled. Enable “clr enabled” configuration option. Could not use view or function ‘dbo.fn_ModuleTypeView’ because of binding errors.

To resolve this issue, please run the following SQL command on the database of the new primary replica SQL instance.

```
sp_configure 'show advanced options', 1;
GO
RECONFIGURE;
GO
sp_configure 'clr enabled', 1;
GO
RECONFIGURE;
GO
```

Existing Management Group

Use the following series of tasks when using an existing management group with a SQL 2012 AlwaysOn Availability Group.

Tasks to perform with the existing management group

1. Make sure that all SQL machines hosting your Operations Manager databases are part of the availability group replicas, or add them to it if they are not.
2. Open Management Studio on the SQL Machine hosting the Operations Manager

databases, right click on each database that is going to be part of the availability databases, and for each select its **properties** and select **Options** to change the recovery model to **Full** from the drop down list.

3. Note the name and the port of the availability group listener.
4. On each management server run `regedit` from an elevated CMD, then edit `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\System Center\2010\Common\Database`.
Change the `DatabaseServerName` to `<AvailabilityGroupListenerName,portNumber>`
5. On each management server, edit the following file:
`%ProgramFiles%\System Center 2012\Operations Manager\Server\ConfigService.config`
In the `<Category>` tag named "Cmdb", change the value for **ServerName** to the name of the availability group listener and change the **PortNumber** to the availability group listener port.
6. Update the Operations Manager database with the group listener name and port by following these steps:
 - a. Open SQL Server Management Studio.
 - b. Expand Databases, Operations Manager, and Tables.
 - c. Right-click `dbo. MT_Microsoft$SystemCenter$ManagementGroup`, and then click **Edit Top 200 Rows**.
 - d. Change the value in the `SQLServerName_<GUID>` column to reflect the `<name,port>` of the availability group listener.
 - e. Save the change.
7. Update the Operations Manager database with the availability group listener to specify the location of the application performance monitoring tables.
 - a. Open SQL Server Management Studio.
 - b. Expand Databases, Operations Manager, and Tables.
 - c. Right-click `dbo. MT_Microsoft$SystemCenter$OpsMgrDB$AppMonitoring`, and then click **Edit Top 200 Rows**.
 - d. Change the value in the `MainDatabaseServerName_<GUID>` column to reflect `<name,port>` of the availability group listener and its port.
 - e. Save the change.
8. Right click each database, and under **Task** select **Back up** (Full Back up).
9. Navigate to the **Availability Group** node and expand it. Right click **Availability database**, and select **Add database**.
On the Select Initial Data Synchronization page, select a data synchronization preference. We recommend selecting **Full**. Full data synchronization has the benefit of creating a full backup and restore of the databases on the secondary replicas.
At the end of this task all databases will be added to the availability database, and restored on all availability replica nodes.
10. Use SQL Server Management Studio to add the databases to the availability databases. Notice that when adding the databases to the availability databases under **Select Data**

Synchronization, three choices are possible: **Full**, **Join only** and **Skip initial data synchronization**. Choose the option that is most appropriate for you. We recommend selecting **Full** and allowing the **Add Database wizard** create a full backup and restore of the databases on the secondary replicas. More steps might or might not be needed depending on which choice you made. See [Manually Prepare a Secondary Database for an Availability Group \(SQL Server\)](#) for more information.

11. For each of the secondary replicas, open **build_mom_db_admin.sql** in notepad. The file is located under <installationMedisFolder>\Setup\AMD64). Then search for the MOMv3 messages section. Copy this section into SQL Server Management Studio, starting and running a new query.

How to Upgrade from the Evaluation Version of Operations Manager

The System Center 2012 – Operations Manager evaluation version expires 180 days after you install it.

To upgrade from an evaluation version of Operations Manager to a licensed version, you must obtain a valid product key from Microsoft. For information about Operations Manager licensing, see [System Center 2012 Licensing](#).



Note

To check whether Operations Manager is licensed, in Operations console, click **Help**, and then click **About**. The version is displayed.

► To upgrade from the evaluation version of Operations Manager to a licensed version

1. On a management server, click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Operations Manager**, and then click **Operations Manager Command Shell**.
2. In the Operations Manager Command Shell, type the following command:
Set-SCOMLicense <license_key>
3. Restart the System Center Data Access Service. You can use the Microsoft Management Console to restart services.
4. Restart the System Center Data Access Service on all management servers in the management group.

For more information about [Set-SCOMLicense](#), type the following in the Operations Manager Command Shell:

```
get-help Set-SCOMLicense
```

For current information about your license, you can use the [Get-SCOMLicense](#) cmdlet. For more information, type the following in the Operations Manager Command Shell:

```
get-help Get-SCOMLicense
```

Installing Operations Manager by Using the Command Prompt Window

You can install features of Operations Manager by using the **setup.exe** command in the Command Prompt window. Gateway and agent installations require the use of MOMGateway.msi and MOMAgent.msi. You must ensure that all servers meet the minimum supported configuration requirements for System Center 2012 – Operations Manager. For more information, see [System Requirements for System Center 2012 - Operations Manager](#).

Command-line Parameters

The following table lists the command-line parameters for installing features of Operations Manager.



Note

If the parameter contains a colon, a value is required. Otherwise, it is simply a switch.

Parameter	Value
/silent	Does not display the installation wizard.
/install	Runs an installation. Use /components to indicate specific features to install.
/InstallPath	Runs an installation specifying an alternative location, to Change the default path for install to another drive. For example: <code>/InstallPath: "D:\Program Files\System Center Operations Manager 2012"</code> to change from the default location of drive C.
/components	OMServer: install a management server. OMConsole: install an Operations console. OMWebConsole: install a web console. OMReporting: install a Reporting server.
/ManagementGroupName:	The name of the management group
/ManagementServicePort:	Change the Management Server port on install
/SqlServerInstance:	The SQL server and instance (<server\instance>).
/DatabaseName:	The name of the Operational database.
/DWSqlServerInstance:	The data warehouse server and instance (<server\instance>).
/DWDatabaseName:	The name of the data warehouse database.

Parameter	Value
/UseLocalSystemActionAccount	Used to specify the Local System for the Management server action account.
/ActionAccountUser:	The domain and user name of the Management server action account. Used if you do not want to specify the Local System
/ActionAccountPassword:	The password for the Management server action account. Used if you do not want to specify the Local System.
/UseLocalSystemDASAccount	Used to specify the Local System for the Data Access service account.
/DASAccountUser:	The domain and user name of the Data Access service account. Used if you do not want to specify the Local System.
/DASAccountPassword:	The password for the Data Access service account. Used if you do not want to specify the Local System.
/DataReaderUser:	The domain and user name of the data reader account.
/DataReaderPassword:	The password for the data reader account.
/DataWriterUser:	The domain and user name of the data writer account.
/DataWriterPassword:	The password for the data writer account.
/EnableErrorReporting:	Never: Do not opt in to sending automatic error reports. Queued: Opt in to sending error reports, but queue the reports for review before sending. Always: Opt in to automatically send error reports.
/SendCEIPReports:	0 : Do not opt in to the Customer Experience Improvement Program (CEIP).

Parameter	Value
	1 : Opt in to CEIP.
/UseMicrosoftUpdate:	0 : Do not opt in to Microsoft Update. 1 : Opt in to Microsoft Update.
/AcceptEndUserLicenseAgreement:	0 : Do not accept the End User License Agreement (EULA). 1 : Accept the End User License Agreement (EULA). When performing a clean installation of System Center 2012 SP1 - Operations Manager, this switch is needed for all management servers. It is also needed for other scripted installations.
/ManagementServer	Used to specify the name of the management server associated with a web console and/or Reporting server that is not installed on a management server.
/WebSiteName:	The name of the website. For default web installation, specify " Default Web Site ". Used for web console installations.
/WebConsoleUseSSL	Specify only if your website has Secure Sockets Layer (SSL) activated. Used for web console installations.
/WebConsoleAuthorizationMode:	Mixed: Used for intranet scenarios. Network: Used for extranet scenarios. Used for web console installations.
/SRSInstance	The reporting server and instance (<server\instance>). Used for Reporting Server installations.
/SendODRReports:	0: Do not opt in to sending operational data reports. 1: opt in to sending operational data reports. Used for Reporting Server Installations.
/uninstall	Uninstalls Operations Manager. Use /components to indicate specific features to uninstall. If /components is not specified, it will uninstall all features of Operations Manager on

Parameter	Value
	the server.

For examples of command lines for installing the various features of Operations Manager see the following:

- [Walkthrough: Installing Operations Manager on a Single Server](#)
- [How to Install the First Management Server in a Management Group](#)
- [How to Install Additional Management Servers](#)
- [How to Install the Operations Console](#)
- [How to Install the Operations Manager Web Console](#)
- [How to Install the Operations Manager Reporting Server](#)
- [How to Deploy a Gateway Server](#)

See Also

[Deploying System Center 2012 - Operations Manager](#)

How to Enable High Availability for the Data Access Service

By default if your Operations Manager Operations console is connected to the Data Access service of one management server and the connection fails, it does not automatically failover to another management server in your management group. To enable high availability for your Operations Manager Data Access service, you can use Network Load Balancing (NLB). By configuring NLB, and connecting to the NLB cluster, if the connection fails, it will automatically be redirected to another management server.

To configure NLB

1. First, you must set up a virtual IP address. You must configure a static IP address for all nodes participating in the cluster and set up DNS. For more information, see. [Configure a Static IP Address](#).
2. You must enable NLB on each management server in your management group. For more information, see
 - [Installing Network Load Balancing](#)
 - [Create a New Network Load Balancing Cluster](#)
 - [Add a Host to the Network Load Balancing Cluster](#)

Using a Firewall

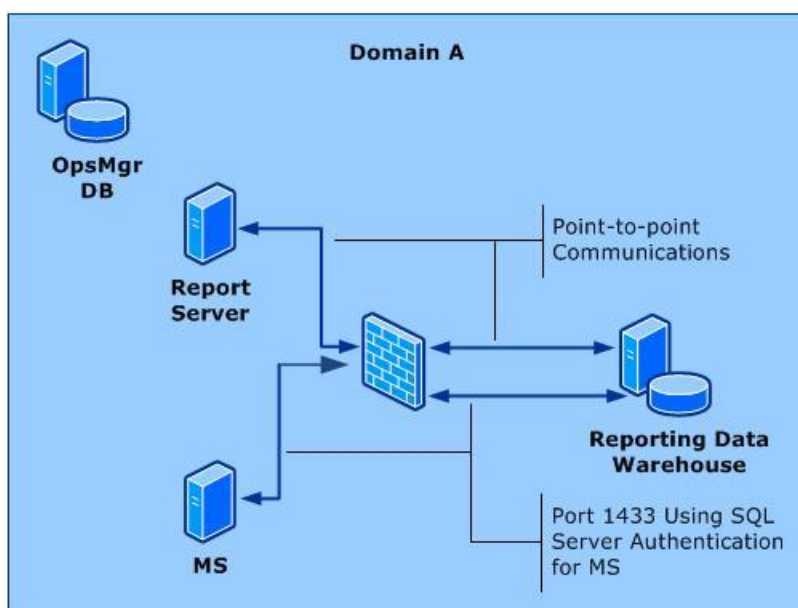
Connecting to the Reporting Data Warehouse Across a Firewall

This section describes how to configure your environment to support the placing of a Report data warehouse behind a firewall.

Note

Separating the Operations console, management server, or Reporting Server by either a firewall or across a trust boundary is not supported.

In an environment where the Reporting data warehouse is separated from the management server and Reporting Server by a firewall, Windows Integrated Authentication cannot be used. You need to take steps to configure SQL Server Authentication. The following sections explain how to enable SQL Server Authentication between the management server (or management server), the Reporting Server, and the Reporting data warehouse, as shown in the following illustration.



Management Server and Reporting Data Warehouse

The following steps are necessary to enable SQL Server Authentication:

1. On the computer hosting the Reporting data warehouse, create a SQL Server Login in the proper role for reader and writer. The credentials you supply for this account must be made a member of the following roles in the data warehouse database on the computer running SQL Server:
 - a. OpsMgrWriter
 - b. db_owner (only for the owning management group in the database)
2. On the computer hosting the management server, create a Run As Account (of type Simple) with the credentials from the previous step.

- Associate this Run As Account with the Run As Profile called Data Warehouse SQL Server Authentication Account, targeting this Run As Profile to each management server. For more information, see [How to Change the Run As Account Associated with a Run As Profile](#) in this guide.

If there is a firewall between the management server and the Reporting data warehouse, you will have to open port 1433.

Reporting Server and Reporting Data Warehouse

If there is a firewall or trust boundary between the Reporting Server and the Reporting data warehouse, point-to-point communications will need to be established.

The account that was specified as the Data Reader Account during setup of Reporting becomes the Execution Account on Reporting Server, and it is this account that will be used to connect to the Reporting data warehouse.

You should determine what port number the computer running SQL Server on the Reporting data warehouse is using and enter this number into the dbo.MT_DataWarehouse table in the Operations Manager database. See [How to Configure the Reporting Data Warehouse to Listen on a Specific TCP/IP Port](#).

Reporting Server and Management Server Separated by a Firewall

A "Could not verify if current user is in sysadmin Role" error message might display when installing Reporting if the reporting server and the management server are separated by a firewall. This error message might display even if the proper firewall ports have been opened. This error occurs after entering the computer name for the management server and clicking **Next**. This error might also display because Reporting Setup was unable to connect to the operational database on the management server. In this environment you must determine what port number is being used by the computer running SQL Server and configure the Operations Manager database to use the port number. See the topic [How to Configure the Operations Manager Database to Listen on a Specific TCP/IP Port](#).

Port Assignments

The following table shows Operations Manager feature interaction across a firewall, including information about the ports used for communication between the features, which direction to open the inbound port, and whether the port number can be changed.

Operations Manager Feature A	Port Number and Direction	Operations Manager Feature B	Configurable	Note
management server	1433 --->	Operations Manager database	Yes (Setup)	
management server	5723, 5724 ---	management	No	Port 5724 must be

Operations Manager Feature A	Port Number and Direction	Operations Manager Feature B	Configurable	Note
	>	server		open to install this feature and can be closed after this feature has been installed.
gateway server	5723 --->	management server	No	
management server	1433 --->	Reporting data warehouse	No	
Reporting server	5723, 5724 --->	management server	No	Port 5724 must be open to install this feature and can be closed after this feature has been installed.
Operations console	5724 --->	management server	No	
Connector framework source	51905 --->	management server	No	
web console server	Web site port --->	management server	No	
web console browser	51908 --->	web console server	Yes (IIS Admin)	Port 51908 is the default port used when selecting Windows Authentication. If you select Forms Authentication, you will need to install an SSL certificate and configure an available port for https functionality for the Operations Manager web console web site.

Operations Manager Feature A	Port Number and Direction	Operations Manager Feature B	Configurable	Note
connected management server (Local)	5724 --->	connected management server (Connected)	No	
Agent installed using MOMAgent.msi	5723 --->	management server	Yes (Setup)	
Agent installed using MOMAgent.msi	5723 --->	management server	Yes (Setup)	
Agent installed using MOMAgent.msi	5723 --->	gateway server	Yes (Setup)	
gateway server	5723 --->	management server	Yes (Setup)	
Agent (Audit Collection Services forwarder)	51909 --->	management server Audit Collection Services collector	Yes (Registry)	
Agentless Exception Monitoring data from client	51906 --->	management server Agentless Exception Monitoring file share	Yes (Client Monitoring Wizard)	
Customer Experience Improvement Program data from client	51907 --->	management server (Customer Experience Improvement Program End) Point	Yes (Client Monitoring Wizard)	
Operations console (reports)	80 --->	SQL Reporting Services	No	The Operations console uses Port 80 to connect to the SQL Reporting Services web site.

Operations Manager Feature A	Port Number and Direction	Operations Manager Feature B	Configurable	Note
Reporting server	1433 --->	Reporting data warehouse	Yes	
management server (Audit Collection Services collector)	1433 --->	Audit Collection Services database	Yes	

How to Configure the Operations Manager Database to Listen on a Specific TCP/IP Port

Perform the following steps to configure a static port for the operational database:

- Use the SQL Server Configuration Manager to disable dynamic port addressing, specify a static port, disable and stop the SQL Server Browser service, and then restart the SQL Server <Instance> service.
- Edit the dbo.MT_ManagementGroup table with the static port number.
- Edit the registry to configure the static port number on the management server.

Caution

Incorrectly editing the registry can severely damage your system. Before making changes to the registry, you should back up any important data.

To configure the operational database port number

1. Log on to the computer hosting the operational database.
2. On the Windows desktop, click **Start**, point to **Programs**, point to the appropriate offering of Microsoft SQL Server, point to **Configuration Tools**, and then click **SQL Server Configuration Manager**.
3. In the **SQL Server Configuration Manager** dialog box, expand **SQL Server Network Configuration**, and then click **Protocols for <INSTANCE>**.
4. In the results pane, right-click **TCP/IP**, and then click **Properties**.
5. In the **TCP/IP Properties** dialog box, click the **IP Addresses** tab.
6. Several IP addresses appear in the format **IP1**, **IP2**, up to **IPAll**. One of these is for the IP address of the loopback adapter, 127.0.0.1. Additional IP addresses appear for each IP address on the computer. Expand **IP1**, **IP2**, up to **IPAll**.
7. For the **IP_n** areas, if the **TCP Dynamic Ports** dialog box contains a **0**, indicating the Database Engine is listening on dynamic ports, delete the **0**.
8. In the **IPAll** area, if the **TCP Dynamic Ports** dialog box contains a port number (which indicates the dynamic port number that was assigned), delete the port number.
9. In the **IPAll** area, in the **TCP Port** dialog box, enter the static port number you want to

use, and then click **OK**.

10. In the **SQL Server Configuration Manager** dialog box, click **SQL Server Services**.
11. In the **SQL Server Configuration Manager** results pane, right-click **SQL Server Browser**, and select **Properties**.
12. In the **SQL Server Browser Properties** dialog box, click the **Service** tab.
13. In the Service tab, click **Start Mode**. In the **Start Mode** list, click **Disabled**, and then click **OK**.
14. In the SQL Server Configuration Manager results pane, right-click **SQL Server Browser**, and then click **Stop**.
15. In the results pane, right-click **SQL Server (<instance name>)**, and then click **Restart**.
16. Close the **SQL Server Configuration Manager**.

▶ **To enter the SQL Server port number into the dbo.MT_ManagementGroup table**

1. On the computer hosting the operational database, on the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server type** list, select **Database Engine**.
3. In the **Server name** list, type the server name, instance, and port number for your operational database (for example, computer\- 4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
- 5. In the Object Explorer pane, expand **Databases**, expand the operational database (for example, **OperationsManager**), expand **Tables**, right-click **dbo.MT_ManagementGroup**, and then click **Open Table**.
- 6. In the results pane, scroll to the right to the column titled **SQLServerName_<guid>**.
- 7. In the first row, enter computer\computer\INSTANCE1, <port>).
- 8. Click **File**, and then click **Exit**.

▶ **To edit the registry on the management server**

1. Log on to the computer hosting the management server.
2. On the Windows desktop, click **Start**, click **Run**, type **regedit**, and then click **OK**.
3. On the **Registry Editor** page, expand **HKEY_LOCAL_MACHINE**, expand **SOFTWARE**, expand **Microsoft**, expand **Microsoft Operations Manager**, expand **3.0**, and then click **Setup**.
4. In the results pane, right-click **DatabaseServerName**, and then click **Modify**.
5. In the **Edit String** dialog box, in the Value data text box, append the database server name entry with a comma and a space, and then type the port number. For example, **<comuter_name>\<instance>, <port number>**.
6. Click **OK**.

How to Configure the Reporting Data Warehouse to Listen on a Specific TCP/IP Port

Perform the following procedures to configure a static port for the Reporting data warehouse:

- Use the SQL Server Configuration Manager to disable dynamic port addressing, specify a static port, disable and stop the SQL Server Browser service, and then restart the SQL Server <Instance> service.
- Edit the dbo.MT_ManagementGroup table with the static port number.
- Edit the dbo.MemberDatabase table with the static port number.
- Edit the registry to configure the static port number on the management server.

Caution

- Incorrectly editing the registry can severely damage your system. Before making changes to the registry, you should back up any important data.
- Edit the SQL Server Reporting Services settings.

To configure the Operations Manager database port number

1. Log on the computer hosting the Reporting data warehouse.
2. On the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, point to **Configuration Tools**, and then click **SQL Server Configuration Manager**.
3. In the **SQL Server Configuration Manager** dialog box, expand **SQL Server 2008 Network Configuration**, and then click **Protocols for <INSTANCE>**.
4. In the results pane, right-click **TCP/IP**, and then click **Properties**.
5. In the **TCP/IP Properties** dialog box, click the **IP Addresses** tab.
6. Several IP addresses appear in the format **IP1**, **IP2**, up to **IPAll**. One of these is for the IP address of the loopback adapter, 127.0.0.1. Additional IP addresses appear for each IP Address on the computer. Expand **IP1**, **IP2**, up to **IPAll**.
7. For the **IP_n** areas, if the **TCP Dynamic Ports** dialog box contains a **0**, indicating the Database Engine is listening on dynamic ports, delete the **0**.
8. In the **IPAll** area, if the **TCP Dynamic Ports** box contains a port number (which indicates the dynamic port number that was assigned) delete the port number.
9. In the **IPAll** area, in the **TCP Port** dialog box, enter the static port number you want to use, and then click **OK**.
10. In the **SQL Server Configuration Manager** dialog box, click **SQL Server 2008 Services**.
11. In the **SQL Server Configuration Manager** results pane, right-click **SQL Server Browser** and select **Properties**.
12. In the **SQL Server Browser Properties** dialog box, click the **Service** tab.
13. On the Service tab, click **Start Mode**. In the **Start Mode** list, click **Disabled**, and then click **OK**.
14. In the SQL Server Configuration Manager results pane, right-click **SQL Server Browser**,

and then click **Stop**.

15. In the results pane, right-click **SQL Server (<instance name>)** and then click **Restart**.
16. Close the **SQL Server Configuration Manager**.

▶ **To enter the SQL Server port number into the dbo.MT_ManagementGroup table**

1. On the computer hosting the operational database, on the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server type** list, select **Database Engine**.
3. In the **Server name** list, type the server and instance for your operational database (for example, computer\INSTANCE1).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the Object Explorer pane, expand **Databases**, expand **OperationsManager** (or the name of the operational database if the default name was not used), expand **Tables**, right-click **dbo.MT_DataWarehouse**, and then click **Open Table**.
6. In the results pane, scroll to the right to the column titled **MainDatabaseServerName_<guid>**.
7. In the first row, enter computer\<instance> followed by a comma, a space, and then the SQL Server port number (for example, **computer\<instance>, <port>**).
8. Click **File**, and then click **Exit**.

▶ **To enter the SQL Server port number into the dbo.MemberDatabase table**

1. On the computer hosting the Reporting data warehouse, on the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server type** list, select **Database Engine**.
3. In the **Server name** list, type the server and instance for your operational database (for example, **computer\<instance>**).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the Object Explorer pane, expand **Databases**, expand **OperationsManagerDW** (or the name of the data warehouse if you did not use the default name), expand **Tables**, right-click **dbo.MemberDatabase**, and then click **Open Table**.
6. In the results pane, scroll to the right to the column titled **ServerName**.
7. In the first row, enter computer\<instance> followed by a comma, a space, and then the SQL Server port number (for example, **computer\<instance>, <port>**).
8. Click **File**, and then click **Exit**.

▶ **To edit the registry on the Reporting Server**

1. Log on to the computer hosting the management server.
2. On the Windows desktop, click **Start**, click **Run**, type **regedit**, and then click **OK**.

3. On the **Registry Editor** page, expand **HKEY_LOCAL_MACHINE**, expand **SOFTWARE**, expand **Microsoft**, expand **Microsoft Operations Manager**, expand **3.0**, and then click **Reporting**.
4. In the results pane, right-click **DWDBInstance**, and then click **Modify**.
5. In the **Edit String** dialog box, in the Value data text box, append the database server name entry with a comma and a space, and then type the port number. For example, **<computer_name>\<instance>, <port number>**.
6. Click **OK**.

 **To edit SQL Server Reporting Services**

1. Log on to the computer hosting the management server.
2. Start Internet Explorer and connect to `http://<computer name>/reports$<instance name>`.
3. Click the **Contents** tab.
4. On the right side of the toolbar, click **Show Details**.
5. Click **Data Warehouse Main**.
6. In the **Connection string** text box, locate the line that reads **source=<computer>\<instance>;initial**.
7. Append the instance name with a comma and a space, and then type the static port number. For example, **source=<computer>\<instance>, <port>;initial**.
8. Click **Apply**, and then close the browser.

Upgrading to System Center 2012 - Operations Manager

This section of the Deployment Guide provides information about how to upgrade to System Center 2012 – Operations Manager from System Center Operations Manager 2007 R2.

If you are upgrading from System Center 2012 – Operations Manager to System Center 2012 Service Pack 1 (SP1), Operations Manager, see the procedures for SP1 in **Upgrading System Center 2012 – Operations Manager to System Center 2012 SP1**

 **Important**

This is the only supported upgrade path to System Center 2012 – Operations Manager. If you are using another, you must first upgrade to System Center Operations Manager 2007 R2.

See Also

[Upgrading from System Center Operations Manager 2007 R2](#)

Upgrading from System Center Operations Manager 2007 R2

This section of the Deployment Guide provides information about how to upgrade from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager. This section of the guide is not intended to be read in order, from start to finish, because your upgrade path will depend on your current configurations. You should use the [Upgrade Process Flow Diagrams](#) or [Upgrade Path Checklists for Operations Manager](#) to help guide you through the upgrade process.

Upgrading to System Center 2012 – Operations Manager is supported from Operations Manager 2007 R2 CU4, or from the latest available CU. Before you begin the upgrade process, make sure that all the servers in the management group meet the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#). If a server does not meet the minimum supported configurations, you might have to introduce new servers into your management group before you upgrade. For more information, see [Upgrading Hardware and Software to Meet System Requirements](#).

When you run upgrade on an Operations Manager 2007 R2 management group, the Upgrade wizard automatically detects the Operations Manager 2007 R2 features that are installed, and it lists the features that will be upgraded. For example, on an Operations Manager 2007 R2 single-server management group with all the features installed, the Upgrade wizard lists the operational database, management server, data warehouse, operations console, web console, and reporting. The System Center 2012 – Operations Manager Upgrade wizard performs system prerequisite checks and provides resolution steps for any issues. Installation will not continue until you resolve all issues. If any of the mandatory Operations Manager features were not previously installed in the Operations Manager 2007 R2 management group, such as the data warehouse, the Upgrade wizard automatically detects the feature and adds it to the list of features to be added during the upgrade process.

In System Center 2012 – Operations Manager, all management servers are peers; there is no root management server (RMS). Therefore, the RMS is no longer a single point of failure as all management servers host the services previously hosted only by the RMS. Roles are distributed to all the management servers. If one management server becomes unavailable, its responsibilities are automatically redistributed.

If you are upgrading a distributed management group, you must upgrade certain features, such as the secondary management servers, gateways, and agents before you upgrade the management group. You run the management group upgrade from the server that hosts the RMS, unless it does not meet the minimum supported configurations for System Center 2012 – Operations Manager. For example, if the RMS is installed on a 32-bit operating system or if it is a clustered RMS, you cannot run upgrade from the RMS. Instead, you must upgrade the management group from a secondary management server. If you follow this upgrade path, this secondary management server is marked as the RMS emulator, and the unsupported RMS is removed from the management group. The RMS emulator enables legacy management packs that rely on the RMS to continue to function in System Center 2012 – Operations Manager. For

more information about the supported configurations for System Center 2012 – Operations Manager, see [Supported Configurations for System Center 2012 – Operations Manager](#).



Note

If you upgrade from the secondary management server, you can build a new management server with the same Windows computer name as the old RMS, rather than change the configuration settings to point to the new management server.

There are four upgrade paths. The path you choose depends on your current topology and system configurations. The following table describes the upgrade paths in more detail.

Upgrade Paths	Description
Single-server Upgrade (Simple)	Use this upgrade path when you have an Operations Manager 2007 R2 management group where all features are installed on the same server, and the hardware and software meets the minimum supported configuration for System Center 2012 – Operations Manager.
Single-server Upgrade (Complex)	Use this upgrade path when you have an Operations Manager 2007 R2 management group where all features are installed on the same server, and the hardware and software do not meet the minimum supported configuration for System Center 2012 – Operations Manager. If the operating system on the server is 32-bit, a new, 64-bit server is required.
Distributed Upgrade (Simple)	Use this path when you have an Operations Manager 2007 R2 management group where various features are installed on separate servers, all of which meet the minimum supported configurations for System Center 2012 – Operations Manager.
Distributed Upgrade (Complex)	Use this path when you have an Operations Manager 2007 R2 management group where various features are installed on separate servers, and where one or more servers do not meet the minimum supported configuration for System Center 2012 – Operations Manager. For example, if the RMS is clustered, you must follow this path. If the operating system on any of the server is 32-bit, new 64-bit replacement

Upgrade Paths	Description
	servers are required.

This guide also contains the specific pre-upgrade and post-upgrade procedures and checklists to help you through the upgrade process. The following content will help you upgrade to System Center 2012 – Operations Manager.

- [Upgrade Path Checklists for Operations Manager](#)
- [Upgrading Hardware and Software to Meet System Requirements](#)
- [Pre-Upgrade Tasks for Operations Manager](#)
- [Upgrade Tasks for Operations Manager](#)
- [Improving Upgrade Performance](#)
- [Upgrading a Single-Server Operations Manager 2007 R2 Environment](#)
- [Upgrading a Distributed Operations Manager 2007 R2 Environment](#)
- [Post-Upgrade Tasks when Upgrading from Operations Manager 2007 R2](#)

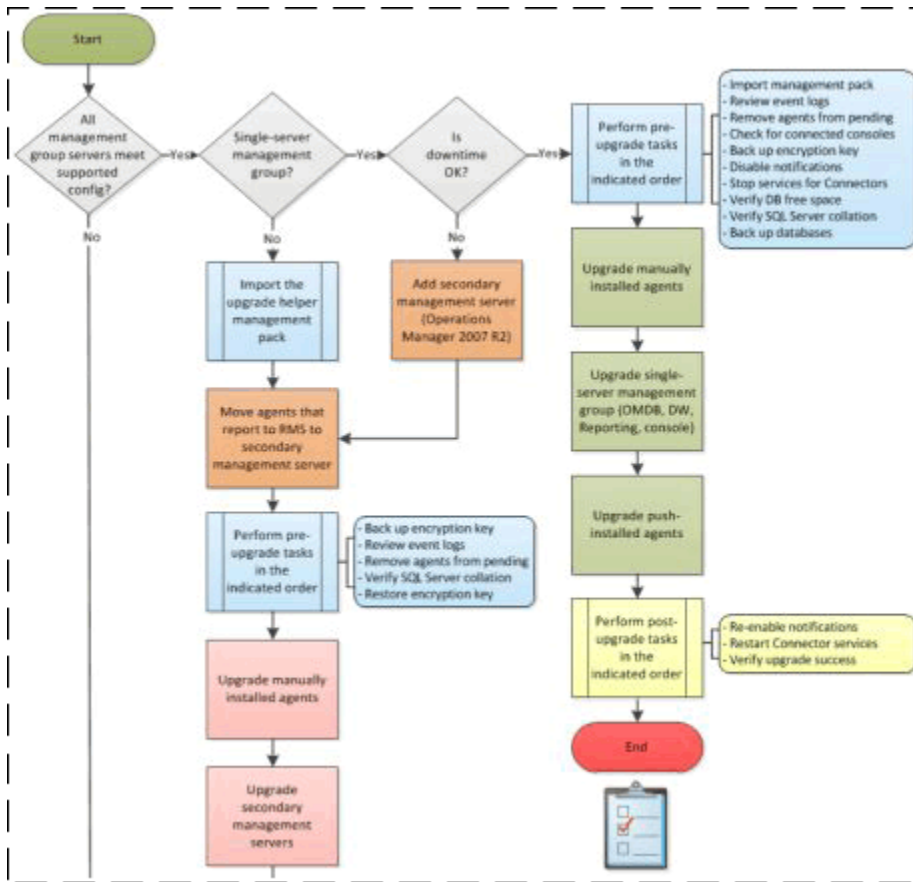
See Also

[Upgrading to System Center 2012 - Operations Manager](#)

Upgrade Process Flow Diagrams

Before you upgrade to System Center 2012 – Operations Manager, you must first determine whether all servers in your System Center Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#). You can use a set of process flow diagrams to determine your upgrade path and visualize the process.

Upgrade process flow diagram



Note

You can click the appropriate process box to open and review the content for any step in the process.

The following table lists the process flow diagrams available, along with a description of when each upgrade path should be used.

Condition	Process flow diagram
When you have a single-server or distributed management group that already meets the minimum supported configuration requirements for System Center 2012 – Operations Manager.	Single-Server and Distributed Upgrade (Simple) Process Flow Diagram
When your single-server management group does not yet meet the minimum supported configuration requirements for System Center 2012 – Operations Manager, and requires new hardware.	Single-Server Upgrade (Complex) Process Flow Diagram

Condition	Process flow diagram
When your distributed management group has one or more servers that do not meet the minimum supported configuration requirements for System Center 2012 – Operations Manager, and might require new hardware.	Distributed Upgrade (Complex) Process Flow Diagram

See Also

[Checklist: Single-Server Upgrade \(Simple\)](#)

[Checklist: Single-Server Upgrade \(Complex\)](#)

[Checklist: Distributed Upgrade \(Simple\)](#)

[Checklist: Distributed Upgrade \(Complex\)](#)

Upgrade Path Checklists for Operations Manager

Use the following checklists to help guide you through an upgrade of System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager. In the table, use the list of conditions to identify the checklist that matches your upgrade path. Essentially, the “simple” path is used when your Operations Manager 2007 R2 management group already meets the supported configuration requirements for System Center 2012 – Operations Manager. The “complex” path is used when your Operations Manager 2007 R2 management group does not yet meet the supported configuration requirements for System Center 2012 – Operations Manager.

 **Important**

Before you follow any of these procedures, make sure that you have verified that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you will need to add any new servers to your management group prior to upgrading. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

Condition	Upgrade Path Checklist
Your Operations Manager 2007 R2 single-server management group already meets the minimum supported configuration requirements for System Center 2012 – Operations Manager.	Checklist: Single-Server Upgrade (Simple)
Your Operations Manager 2007 R2 single-server management group does not meet the minimum supported configuration requirements for System Center 2012 – Operations Manager	Checklist: Single-Server Upgrade (Complex)

Condition	Upgrade Path Checklist
and requires new hardware.	
Your Operations Manager 2007 R2 distributed management group already meets the minimum supported configuration requirements System Center 2012 – Operations Manager.	Checklist: Distributed Upgrade (Simple)
Your Operations Manager 2007 R2 distributed management group has one or more servers that do not meet the minimum supported configuration requirements for System Center 2012 – Operations Manager and might require new hardware.	Checklist: Distributed Upgrade (Complex)

See Also

[Single-Server and Distributed Upgrade \(Simple\) Process Flow Diagram](#)

[Single-Server Upgrade \(Complex\) Process Flow Diagram](#)

[Distributed Upgrade \(Complex\) Process Flow Diagram](#)

Checklist: Single-Server Upgrade (Simple)

This checklist walks you through an upgrade of a System Center Operations Manager 2007 R2 single-server management group that already meets the minimum supported configurations for Operations Manager. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

If your single-server management group does not yet meet the minimum supported configurations for System Center 2012 – Operations Manager, or if you have a distributed management group, see the following checklists.

Upgrade Path Checklist	Condition
Checklist: Single-Server Upgrade (Complex)	Your Operations Manager 2007 R2 single-server management group does not meet the minimum supported configurations for System Center 2012 – Operations Manager and requires new hardware.
Checklist: Distributed Upgrade (Simple)	Your Operations Manager 2007 R2 distributed management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.
Checklist: Distributed Upgrade (Complex)	Your Operations Manager 2007 R2 distributed management group has one or more servers

Upgrade Path Checklist	Condition
	that do not meet the minimum supported configurations for System Center 2012 – Operations Manager and might require new hardware.

If you prefer to avoid downtime on your single-server management group, you can add a secondary management server and then follow the distributed management group upgrade process. For more information, see:

- [How to Add an Operations Manager 2007 R2 Secondary Management Server \(Operations Manager Upgrade\)](#)
- [Checklist: Distributed Upgrade \(Simple\)](#)

Checklist

Use the following checklist to upgrade your single-server management group if it already meets the supported configuration requirements for System Center 2012 – Operations Manager



Tip

You can also view a process flow diagram that links to the relevant topics. For more information, see [Single-Server and Distributed Upgrade \(Simple\) Process Flow Diagram](#)

	Task	References
<input type="checkbox"/>	Import the Upgrade Helper management pack.	Import the Upgrade Helper Management Pack
<input type="checkbox"/>	Review the Operations Manager 2007 R2 event logs.	Review the Operations Manager 2007 R2 Event Logs
<input type="checkbox"/>	Remove agents from Pending Management.	Remove Agents from Pending Management
<input type="checkbox"/>	Check for any active connected consoles to the root management server.	Check the Operations Manager 2007 R2 RMS for Active Connected Consoles
<input type="checkbox"/>	Back up the RMS encryption key (SecureStorageBackup.exe).	Back Up the RMS Encryption Key
<input type="checkbox"/>	Disable all notification subscriptions.	Disable Notification Subscriptions
<input type="checkbox"/>	Stop services or disable any connectors that are installed.	Stop Services for Connectors
<input type="checkbox"/>	Verify that your operational database has enough free space.	Verify that the Operational Database Has More than 50

	Task	References
		Percent of Free Space
<input type="checkbox"/>	Verify that you have a supported SQL Server collation on all databases and instances of databases.	Verify the SQL Server Collation
<input type="checkbox"/>	Back up the databases.	Back up the Operations Manager Databases
<input type="checkbox"/>	Upgrade the manually installed agents.	Upgrading Manually Installed Agents
<input type="checkbox"/>	Run the management group upgrade on the root management server.	How to Upgrade an Operations Manager 2007 R2 Single-Server Management Group
<input type="checkbox"/>	Upgrade the push-installed agents.	Upgrading Push-Installed Agents
<input type="checkbox"/>	Re-enable the notification subscriptions.	Re-enable the Notification Subscriptions.
<input type="checkbox"/>	Restart or re-enable the service for any connectors that are installed.	Restart the Connector Services
<input type="checkbox"/>	Update overrides.	Update Overrides
<input type="checkbox"/>	Verify the success of the upgrade.	Verify upgrade success

See Also

[Upgrade Path Checklists for Operations Manager Single-Server and Distributed Upgrade \(Simple\)](#)

Checklist: Single-Server Upgrade (Complex)

This checklist walks you through an upgrade of a System Center Operations Manager 2007 R2 single-server management group that does not meet the supported configuration requirements for System Center 2012 – Operations Manager, and requires new hardware. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

If your single-server management group already meets the minimum supported configurations for System Center 2012 – Operations Manager, or if you have a distributed management group, see the following checklists.

Upgrade Path Checklist	Condition
Checklist: Single-Server Upgrade (Simple)	Your Operations Manager 2007 R2 single-server management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.
Checklist: Distributed Upgrade (Simple)	Your Operations Manager 2007 R2 distributed management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.
Checklist: Distributed Upgrade (Complex)	Your Operations Manager 2007 R2 distributed management group has one or more servers that do not meet the minimum supported configurations for System Center 2012 – Operations Manager and might require new hardware.

Checklist

Use the following checklist to upgrade your single-server management group if it does not yet meet the supported configuration requirements for System Center 2012 – Operations Manager.



Tip

You can also view a process flow diagram that links to the relevant topics. For more information, see [Single-Server Upgrade \(Complex\)](#)

	Task	References
<input type="checkbox"/>	Add a secondary management server and install System Center Operations Manager 2007 R2.	How to Add an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
<input type="checkbox"/>	Move agents that report to the root management (RMS) server to the secondary management server.	How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
<input type="checkbox"/>	If SQL Server does not meet the supported configuration requirements, upgrade SQL Server.	Upgrading SQL Server (Operations Manager Upgrade)
<input type="checkbox"/>	Back up the encryption key.	Back Up the Encryption Key

	Task	References
<input type="checkbox"/>	Review the Operations Manager 2007 R2 event logs.	Review the Operations Manager 2007 R2 Event Logs
<input type="checkbox"/>	Remove agents from Pending Management.	Remove Agents from Pending Management
<input type="checkbox"/>	Verify that you have a supported SQL Server collation on all databases and instances of databases.	Verify the SQL Collation
<input type="checkbox"/>	Upgrade the manually installed agents.	Upgrading Manually Installed Agents
<input type="checkbox"/>	Upgrade the secondary management server.	How to Upgrade a Secondary Management Server from Operations Manager 2007 R2
<input type="checkbox"/>	Upgrade the push-installed agents.	Upgrading Push-Installed Agents
<input type="checkbox"/>	Check for any active connected consoles to the root management server.	Check the Operations Manager 2007 R2 RMS for Active Connected Consoles
<input type="checkbox"/>	Disable all notification subscriptions.	Disable the Notification Subscriptions
<input type="checkbox"/>	Stop services or disable any connectors that are installed.	Stop the Services for Connectors
<input type="checkbox"/>	Verify that your operational database has enough free space.	Verify that the Operational Database Has More than 50 Percent of Free Space
<input type="checkbox"/>	Back up the databases.	Back Up the Operations Manager Databases
<input type="checkbox"/>	Restore the encryption key on secondary management server.	Restore the Encryption Key on the Secondary Management Server
<input type="checkbox"/>	Run management group upgrade on the secondary management server.	How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server
<input type="checkbox"/>	Re-enable the notification	Re-enable the Notification

	Task	References
	subscriptions.	Subscriptions.
<input type="checkbox"/>	Restart or re-enable the service for any connectors that are installed.	Restart the Connector Services
<input type="checkbox"/>	Uninstall the old root management server.	Uninstall the Old RMS
<input type="checkbox"/>	Update overrides.	Update Overrides
<input type="checkbox"/>	Verify the success of the upgrade.	Verify the Upgrade Success

See Also

[Upgrade Path Checklists for Operations Manager Single-Server Upgrade \(Complex\)](#)

Checklist: Distributed Upgrade (Simple)

This checklist walks you through an upgrade of a System Center Operations Manager 2007 R2 distributed management group that meets the supported configuration requirements for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

If your distributed management group does not yet meet the minimum supported configurations for System Center 2012 – Operations Manager, or if you have a single-server management group, see the following checklists.

Upgrade Path Checklist	Condition
Checklist: Single-Server Upgrade (Simple)	Your Operations Manager 2007 R2 single-server management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.
Checklist: Single-Server Upgrade (Complex)	Your Operations Manager 2007 R2 single-server management group does not meet the minimum supported configurations for System Center 2012 – Operations Manager and requires new hardware.
Checklist: Distributed Upgrade (Complex)	Your Operations Manager 2007 R2 distributed management group has one or more servers that do not meet the minimum supported configurations for System Center 2012 –

Upgrade Path Checklist	Condition
	Operations Manager and might require new hardware.

Checklist

Use the following checklist to upgrade your distributed management group if it already meets the supported configuration requirements for System Center 2012 – Operations Manager.



Tip

You can also view a process flow diagram that links to the relevant topics. For more information, see [Single-Server and Distributed Updated \(Simple\)](#).



Note

In this checklist, we recommend that you move agents that report to the root management server (RMS) to a secondary management server before upgrading the agents. However, if you do not mind experiencing downtime, you can upgrade the agents after you upgrade the management group instead of moving them to a secondary management server.

	Task	References
<input type="checkbox"/>	Import the Upgrade Helper management pack.	Import the Upgrade Helper Management Pack
<input type="checkbox"/>	Move agents that report to the RMS to a secondary management server.	How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
<input type="checkbox"/>	Back up the encryption key.	Back Up the Encryption Key
<input type="checkbox"/>	Review the Operations Manager 2007 R2 event logs.	Review the Operations Manager 2007 R2 Event Logs
<input type="checkbox"/>	Remove agents from pending management.	Remove Agents from Pending Management
<input type="checkbox"/>	Verify that you have a supported SQL Server collation on all databases and instances of databases.	Verify the SQL Collation
<input type="checkbox"/>	Upgrade the manually installed agents.	Upgrading Manually Installed Agents
<input type="checkbox"/>	Upgrade the secondary	How to Upgrade a Secondary

	Task	References
	management servers.	Management Server from Operations Manager 2007 R2
<input type="checkbox"/>	Upgrade gateways, if present.	How to Upgrade a Gateway Server from Operations Manager 2007 R2
<input type="checkbox"/>	Upgrade the push-installed agents.	Upgrading Push-Installed Agents
<input type="checkbox"/>	Check for any active, connected consoles to the root management server.	Check the Operations Manager 2007 R2 RMS for Active, Connected Consoles
<input type="checkbox"/>	Disable all notification subscriptions.	Disable the Notification Subscriptions
<input type="checkbox"/>	Stop services or disable any connectors that are installed.	Stop the Services for Connectors
<input type="checkbox"/>	Verify that your operational database has enough free space.	Verify that the Operational Database Has More than 50 Percent of Free Space
<input type="checkbox"/>	Back up the databases.	Back Up the Operations Manager Databases
<input type="checkbox"/>	Restore the encryption key on secondary management server.	Restore the Encryption Key on the Secondary Management Server
<input type="checkbox"/>	Run management group upgrade on the root management server.	How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS
<input type="checkbox"/>	Upgrade or install the optional features, such as the web consoles and Reporting server.	Upgrading or Installing Optional Features
<input type="checkbox"/>	Re-enable notification subscriptions.	Re-enable the Notification Subscriptions
<input type="checkbox"/>	Restart or re-enable the service for any connectors that are installed.	Restart the Connector Services
<input type="checkbox"/>	Update overrides.	Update Overrides

	Task	References
<input type="checkbox"/>	Verify the success of the upgrade.	Verify the Upgrade Success

See Also

[Upgrade Path Checklists for Operations Manager Single-Server and Distributed Updated \(Simple\)](#)

Checklist: Distributed Upgrade (Complex)

To upgrade a distributed System Center Operations Manager 2007 R2 management group to System Center 2012 – Operations Manager, you use a phased approach, starting with the management servers, then the gateway servers, and then the management group. The order in which you upgrade the agents depends on how they were deployed (manually installed or push-installed), and whether your root management server (RMS) meets the supported configuration requirements for System Center 2012 – Operations Manager. For example, a clustered RMS is not supported in System Center 2012 – Operations Manager. You also must perform a number of pre-upgrade and post-upgrade tasks, and might perform some optional upgrade tasks.

If any of the servers in your distributed management group do not meet the supported configuration requirements for System Center 2012 – Operations Manager, and require the installation of a new server, you should follow this checklist. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#). Some of the servers might meet these requirements, and therefore, you might not have to perform the steps in every section. For example, if the server that hosts your RMS meets the supported configuration requirements, you can run the final upgrade from the RMS and skip the section on running the final upgrade from a secondary management server.

If your distributed management group already meets the minimum supported configurations for System Center 2012 – Operations Manager, or if you have a single-server management group, see the following topics.

Upgrade Path Checklist	Condition
Checklist: Single-Server Upgrade (Simple)	Your Operations Manager 2007 R2 single-server management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.
Checklist: Single-Server Upgrade (Complex)	Your Operations Manager 2007 R2 single-server management group does not meet the minimum supported configurations for System Center 2012 – Operations Manager and requires new hardware.
Checklist: Distributed Upgrade (Simple)	Your Operations Manager 2007 R2 distributed

Upgrade Path Checklist	Condition
	management group already meets the minimum supported configurations for System Center 2012 – Operations Manager.

Checklist

Use the following checklist to upgrade your distributed management group if any of the servers do not yet meet the supported configuration requirements for System Center 2012 – Operations Manager.



Tip

You can also view a process flow diagram that links to the relevant topics. For more information, see [Distributed Upgrade \(Complex\)](#).

This checklist contains multiple paths and you will not have to follow each step consecutively. For example, you will upgrade the management group from either the RMS or the secondary management server, depending on your current configuration. You should follow the steps in each as needed.

Section	Description
Import the Upgrade Helper Management Pack	Use these procedures to import and use the Upgrade Helper management pack.
Replacing Secondary Management Servers	Use these procedures if your secondary management servers do not meet the minimum system requirements for System Center 2012 – Operations Manager. If your secondary management servers have a 32-bit operating system, you must replace each server. For each 32-bit secondary management server, you must add a new 64-bit server and move the agents from the old management server to the new management server. You must ensure that all management servers meet all of the minimum system requirements for System Center 2012 – Operations Manager.
Replacing Gateways	Use these procedures if your gateway servers do not meet the minimum system requirements for System Center 2012 – Operations Manager. If your gateways have a 32-bit operating system, you must replace each gateway server with a new gateway server that meets the requirements. You must ensure that all

Section	Description
	gateway servers meet the minimum system requirements for System Center 2012 – Operations Manager.
Secondary Management Server Upgrade	Use these procedures to upgrade the secondary management servers, any gateway servers, and agents.
Management Group Upgrade from RMS	Use these procedures only if your RMS meets the minimum system requirements for System Center 2012 – Operations Manager.
Management Group Upgrade from Secondary Management Server	Use these procedures only if your RMS does not meet the minimum system requirements for System Center 2012 – Operations Manager.

Import the Upgrade Helper Management Pack

The Upgrade Helper management pack helps to guide you through the upgrade process. You should import this management pack before you start the upgrade process for a distributed management group that does not meet the supported configuration requirements for System Center 2012 – Operations Manager.

	Task	References
<input type="checkbox"/>	Import the Upgrade Helper Management Pack	Upgrade Helper Management Pack

Replacing Secondary Management Servers

If your secondary management server already meets the minimum system requirements, go to the [Replacing Gateways](#) section of this checklist. Otherwise, use the following procedures for each secondary management server in your management group.



Note

You only have to add new secondary management servers if your current servers have a 32-bit operating system, which do not meet the supported configuration requirements for System Center 2012 – Operations Manager. Otherwise, just ensure that your secondary management servers meet the remaining supported configuration requirements.

	Task	References
<input type="checkbox"/>	If operating system is 32-bit, add a secondary management server.	How to Add an Operations Manager 2007 R2 Secondary Management Server (Operations

	Task	References
		Manager Upgrade)
<input type="checkbox"/>	Move the Operations Manager 2007 R2 agents to a secondary management server, and remove the old secondary management server.	How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
<input type="checkbox"/>	Ensure that the secondary management server meets the supported configuration requirements for System Center 2012 – Operations Manager.	Supported Configurations for System Center 2012 - Operations Manager

Replacing Gateways

If you do not have gateway servers, or you have gateways that meet the minimum system requirements, go to the [Secondary Management Server Upgrade](#) section of this checklist. Otherwise, use the following procedures for each gateway in your management group.



Note

You only have to add new gateway servers if your current servers are 32-bit, which do not meet the supported configuration requirements for System Center 2012 – Operations Manager. Otherwise, just ensure that your gateway servers meet the remaining supported configuration requirements.

	Task	References
<input type="checkbox"/>	If gateway server does not have a 64-bit operating system, build a new gateway server.	How to Replace an Operations Manager 2007 R2 Gateway that Has an Unsupported Configuration (Operations Manager Upgrade)
<input type="checkbox"/>	Remove the old gateway server.	How to Remove an Operations Manager 2007 R2 Gateway (Operations Manager Upgrade)
<input type="checkbox"/>	Ensure that the gateway server meets the supported configuration requirements for System Center 2012 –	Supported Configurations for System Center 2012 - Operations Manager

	Task	References
	Operations Manager.	

Secondary Management Server Upgrade

Use the following procedures to upgrade your secondary management servers, gateway servers, and agents. Before you upgrade the secondary management server, you must ensure that your root management service (RMS) meets the supported configuration requirements for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#). If the RMS does not meet these configuration requirements, you must move agents that report to the RMS to the secondary management server before you upgrade the second management server. You should also ensure that SQL Server meets the supported configuration requirements.

	Task	References
<input type="checkbox"/>	If RMS does not meet supported configuration requirements for System Center 2012 – Operations Manager, move agents that report to root management server to the secondary management server.	How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)
<input type="checkbox"/>	If Microsoft SQL Server does not meet the supported configuration requirements, upgrade SQL Server.	Upgrading SQL Server (Operations Manager Upgrade)
<input type="checkbox"/>	Back up the encryption key.	Back Up the Encryption Key
<input type="checkbox"/>	Review the Operations Manager 2007 R2 event logs.	Review the Operations Manager 2007 R2 Event Logs
<input type="checkbox"/>	Check if any gateway servers report to an unsupported RMS.	Check for Gateway Servers Reporting to the RMS
<input type="checkbox"/>	Remove agents from Pending Management.	Remove Agents from Pending Management
<input type="checkbox"/>	Verify that you have a supported SQL Server collation on all databases and instances of databases.	Verify the SQL Server Collation
<input type="checkbox"/>	Upgrade the manually installed	Upgrading Manually Installed

	Task	References
	agents.	Agents
<input type="checkbox"/>	Upgrade the secondary management servers.	How to Upgrade a Secondary Management Server from Operations Manager 2007 R2
<input type="checkbox"/>	Upgrade gateway servers, if present.	How to Upgrade a Gateway Server from Operations Manager 2007 R2
<input type="checkbox"/>	Upgrade the push-installed agents.	Upgrading Push-Installed Agents

Management Group Upgrade from RMS

If your RMS does not meet the minimum supported configurations for System Center 2012 – Operations Manager, go to the [Management Group Upgrade from Secondary Management Server](#) section of this checklist. Otherwise, use the following procedures to upgrade your management group from the root management server.



Note

A clustered RMS does not meet the supported configuration requirements for System Center 2012 – Operations Manager.

	Task	References
<input type="checkbox"/>	Check for any active, connected consoles to the root management server.	Check the Operations Manager 2007 R2 RMS for Active Connected Consoles
<input type="checkbox"/>	Disable all notification subscriptions.	Disable the Notification Subscriptions
<input type="checkbox"/>	Stop services or disable any connectors that are installed.	Stop the Services for Connectors
<input type="checkbox"/>	Verify that your operational database has sufficient free space.	Verify that the Operational Database has More than 50 Percent of Free Space
<input type="checkbox"/>	Back up all databases.	Back Up the Operations Manager Databases
<input type="checkbox"/>	Run management group upgrade on the root management server.	How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS

	Task	References
<input type="checkbox"/>	Upgrade optional features.	Upgrading or Installing Optional Features
<input type="checkbox"/>	Re-enable the notification subscriptions.	Re-enable the Notification Subscriptions.
<input type="checkbox"/>	Restart or re-enable the service for any connectors that are installed.	Restart the Connector Services
<input type="checkbox"/>	Update overrides.	Update Overrides
<input type="checkbox"/>	Verify the success of the upgrade.	Verify the Upgrade Success

Management Group Upgrade from Secondary Management Server

If your root management server meets the minimum supported configurations for System Center 2012 – Operations Manager, go to the [Management Group Upgrade from RMS](#) section of this checklist. Otherwise, use the following procedures to upgrade your management group from a secondary management server.



Note

A clustered RMS does not meet the supported configuration requirements for System Center 2012 – Operations Manager.

	Task	References
<input type="checkbox"/>	Check for any active, connected consoles to the root management server.	Check the Operations Manager 2007 R2 RMS for Active, Connected Consoles
<input type="checkbox"/>	Disable all notification subscriptions.	Disable the Notification Subscriptions
<input type="checkbox"/>	Stop services or disable any connectors that are installed.	Stop the Services for Connectors
<input type="checkbox"/>	Verify that your operational database has sufficient free space.	Verify that the Operational Database has More than 50 Percent of Free Space
<input type="checkbox"/>	Back up all databases.	Back Up the Operations Manager Databases
<input type="checkbox"/>	Restore the encryption key.	Restore the Encryption Key on the Secondary Management

	Task	References
		Server
<input type="checkbox"/>	Run the management group upgrade on the secondary management server.	How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server
<input type="checkbox"/>	If required, install the optional features, such as the consoles and Reporting.	Upgrading or Installing Optional Features
<input type="checkbox"/>	Re-enable the notification subscriptions.	Re-enable the Notification Subscriptions.
<input type="checkbox"/>	Restart or re-enable the service for any connectors that are installed.	Restart the Connector Services
<input type="checkbox"/>	Uninstall the old root management server.	Uninstall the Old RMS
<input type="checkbox"/>	Update overrides.	Update Overrides
<input type="checkbox"/>	Verify the success of the upgrade.	Verify the Upgrade Success

See Also

[Upgrade Path Checklists for Operations Manager Distributed Upgrade \(Complex\)](#)

Pre-Upgrade Tasks for Operations Manager

You have to perform a number of pre-upgrade tasks before you upgrade from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager. The order in which you perform these tasks will vary depending on your upgrade path. For more information about which order you should follow, see [Upgrade Path Checklists for Operations Manager](#).

Overview of the Pre-Upgrade Tasks

In a single-server management group upgrade, you must perform all the applicable pre-upgrade tasks before you start the upgrade process. Service will be interrupted until the upgrade process is completed. If your single-server management group does not meet the minimum system requirements, or you do not want to experience downtime, you can add a secondary management server, and then follow the distributed management group upgrade process.

In a distributed management group upgrade, you perform the upgrade in phases to minimize the interruption in service. For more information about these phases, see [Upgrade Tasks for Operations Manager](#). You might have to perform pre-upgrade tasks before each upgrade phase.

 **Important**

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

The following table shows the tasks that you must complete before you upgrade from Operations Manager 2007 R2 to System Center 2012 – Operations Manager. This table provides the following information:

- Tasks to complete
- Links to the procedures related to those tasks
- Potential downtime that a task might create
- Description of the potential risk to the stability of your data and monitoring environment and how to mitigate that risk

 **Important**

The order of the tasks depends on the upgrade path that you follow. Use the [Upgrade Path Checklists for Operations Manager](#) to follow the steps in order for your particular upgrade scenario.

Task	Downtime, risk, and mitigation
Upgrade Hardware and Software to Meet System Requirements	Possible downtime if hardware and software changes are needed. Risk dependent on required changes.
Import the Upgrade Helper Management Pack	No downtime or interference; low risk.
Back up the RMS Encryption Key	No downtime or interference; low risk.
Review the Operations Manager 2007 R2 Event Logs	No downtime or interference; low risk.
Check for Gateway Servers Reporting to the RMS	No downtime or interference; low risk if the management servers have the necessary certificates.
Remove Agents from Pending Management	No downtime or interference; low risk.
Check the Operations Manager 2007 R2 RMS for Active Connected Consoles	Consoles might lose connectivity to the RMS during upgrade.

Task	Downtime, risk, and mitigation
Disable the Notification Subscriptions	<ul style="list-style-type: none"> • Interference; no notifications are sent during the upgrade. • Mitigation; after the upgrade, check for any alerts that were missed.
Stop the Services or Disable any Connectors	Connectors do not function during upgrade.
Verify that the Operational Database Has More Than 50 Percent Free Space	No downtime or interference; low risk.
Verify the SQL Server Collation	The management group upgrade does not succeed if unsupported collation configurations exist.
Back up the Operations Manager Databases	Depending on the backup technology that you use, some backup methods might lock a database during backup.
Restore the RMS Encryption Key on the Secondary Management Server	No downtime or interference; low risk. Required only if the root management server (RMS) does not meet the supported configuration requirements for System Center 2012 – Operations Manager. This should be performed just prior to management group upgrade.
Upgrade SQL Server Reporting Services	The reports will be unavailable, but data will not be lost.

Upgrade Hardware and Software to Meet System Requirements

Before you perform the pre-upgrade and upgrade tasks, you might have to upgrade the hardware and software to meet system requirements. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#) and [Upgrading Hardware and Software to Meet System Requirements](#).

Import the Upgrade Helper Management Pack

An Upgrade Helper management pack is available to help guide you through the upgrade process. For information about how to import and use the Upgrade Helper management pack, see [Upgrade Helper Management Pack](#).

Review the Operations Manager 2007 R2 Event Logs

Review the event logs for Operations Manager 2007 R2 on the root management server (RMS) and on the management servers to look for recurring warning or critical events. Address them and save a copy of the event logs before you perform your upgrade.

Check for Gateway Servers Reporting to the RMS

If there are gateway servers that report to an Operations Manager 2007 R2 RMS with an unsupported configuration, you must ensure that the secondary management server from which you will perform the management group upgrade can communicate with the gateway. You can run a Windows PowerShell script to display the primary and failover management servers for all gateway servers. Run the following script.

```
#Display Primary and Failover Management Servers for all Gateway Servers
$GWs = Get-SCOMManagementServer | where {$_.IsGateway -eq $true}
$GWs | sort | foreach {
Write-Host "";
"Gateway MS :: " + $_.Name;
"--Primary MS :: " + ($_.GetPrimaryManagementServer()).ComputerName;
$failoverServers = $_.getFailoverManagementServers();
foreach ($managementServer in $failoverServers) {
"--Failover MS :: " + ($managementServer.ComputerName);
}
}
Write-Host "";
```

To ensure mutual authentication between the gateway and the secondary management server, you install certificates from a certification authority (CA) on the secondary management server and the gateway server. For more information, see the [Deploying the Certificates](#) section of [How to Replace an Operations Manager 2007 R2 Gateway that Has an Unsupported Configuration \(Operations Manager Upgrade\)](#).

After you have imported the certificates on the new secondary management server, and you verify that the gateway server has a healthy state, you must set the new management server as the primary management server for the gateway, and set the RMS as the secondary management server.

Remove Agents from Pending Management

Before you upgrade the secondary management server, remove any agents that are in Pending Management.

To remove agents that are in Pending Management

1. Log on to the Operations console by using an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 management group.
2. In the **Administration** pane, expand **Device Management**, and then click **Pending Management**.
3. Right-click each agent, and then click **Approve** or **Reject**.

Back up the RMS Encryption Key

The Operations Manager 2007 R2 root management server (RMS) encryption key is necessary to decrypt secure data in the operational database. When you have a backup of the RMS encryption key, you can import the key on a new management server when you upgrade the management group from an Operations Manager 2007 R2 secondary management server.

▶ **To back up the encryption key by using the Encryption Key Backup or Restore Wizard**

1. Log on to the computer hosting the secondary management server with an account that is a member of the Administrators group.
2. Open a command prompt window by using the **Run as Administrator** option.
3. At the command prompt, type:
cd <Operations Manager Installation Folder>
SecureStorageBackup
4. In the **Encryption Key Backup or Restore Wizard**, on the **Backup or Restore** page, select the **Backup the Encryption Key** option, and then complete the wizard, providing a location and password for the key.



Note

Recovery of the password is not possible if the key is lost or forgotten.



Note

Store the encryption key in a location that can be easily accessed, such as a file share. You have to restore this encryption key on all management servers in your management group before you upgrade.

▶ **To back up the RMS encryption key by using the Command Prompt window**

1. Log on to the computer that hosts the Operations Manager 2007 R2 root management server by using an account that is a member of the Administrators group.
2. Open a Command Prompt window as an administrator by using the **Run as administrator** option.
3. At the command prompt, type **cd <path to installation folder>**, and then press Enter.
4. To back up the encryption key, do the following:
 - a. Type **SecureStorageBackup Backup <BackupFile>**, and then press Enter.
 - b. At the **Please enter the password to use for storage/retrieval** prompt, type a password that is at least eight characters long, and then press Enter.
 - c. At the **Please re-enter your password** prompt, type the same password, and then press Enter.

Check the Operations Manager 2007 R2 RMS for Active Connected Consoles

Consoles that are connected to the Operations Manager 2007 R2 RMS might lose connectivity during the upgrade of the management group. Before you perform the upgrade of the management group, you should notify anyone who has a connected console to close the connection.

Disable the Notification Subscriptions

You should disable notification subscription before you upgrade the management group to ensure that notifications are not sent during the upgrade process.

▶ To disable subscriptions

1. Log on to the Operations console account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, select the **Administration** view.
3. In the navigation pane, expand **Administration**, expand the **Notifications** container, and then click **Subscriptions**.
4. Select each subscription, and then click **Disable** in the **Actions** pane.



Note

Multiselect does not work when you are disabling subscriptions.

Stop the Services or Disable any Connectors

Refer to the non-Microsoft connector documentation for any installed Connectors to determine the services used for each Connector, and whether it is supported for System Center 2012 – Operations Manager.

▶ To stop a service for Connectors

1. On the **Start** menu, point to **Administrative Tools**, and then click **Services**.
2. In the **Name** column, right-click the Connector that you want to control, and then click **Stop**.

Verify that the Operational Database Has More Than 50 Percent Free Space

You must verify that the operational database has more than 50 percent of free space before you upgrade the management group because the upgrade might fail if there is not enough space. You should also ensure that the transactions logs are 50 percent of the total size of the operational database.

▶ To check how much free space the Operational Database has

1. On the computer that hosts the operational database, open **SQL Server Management Studio**.
2. In the **Object Explorer**, expand **Databases**.
3. Right-click the operational database, point to **Reports, Standard Reports**, and then click **Disk Usage**.
4. View the **Disk Usage** report to determine the percentage of free space.

▶ To increase the free space for the operational database and log files

1. On the computer that hosts the operational database, open **SQL Server Management Studio**.

2. In the **Connect to Server** dialog box, in the **Server Type** list, select **Database Engine**.
3. In the **Server Name** list, select the server and instance for your operational database (for example, computer\INSTANCE1).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the **Object Explorer** pane, expand **Databases**, right-click the operational database, and then click **Properties**.
6. In the **Database Properties** dialog box, under **Select a page**, click **Files**.
7. In the results pane, increase the **Initial Size** value for the **MOM_DATA** database by 50 percent.



Note

This step is not required if free space already exceeds 50 percent.

8. Set the **Initial Size** value for the **MOM_LOG** to be 50 percent of the total size of the database. For example, if the operational database size is 100 GB, the log file size should be 50 GB. Then click **OK**.

Verify the SQL Server Collation

SQL Server collation for all databases and database instances must be one of the following:

Language	Collation
English	SQL_Latin1_General_CP1_CI_AS
French	French_CI_AS
Russian	Cyrillic_General_CI_AS
Chinese CHS	Chinese_PRC_CI_AS
Japanese	Japanese_CI_AS
Spanish	Traditional_Spanish_CI_AS
Other Languages	Latin1_General_CI_AS



Important

You must ensure that all databases and database instances have the correct collation before you run upgrade on the management group.

To determine the SQL Server collation of a database, you can check the database properties. In SQL Server Management Studio, right-click the database you want to check, and then click **Properties**. The collation is listed under **Maintenance**.

For information about changing the SQL Server collation of a database, see [Setting and Changing the Server Collation](#).

Restore the RMS Encryption Key on the Secondary Management Server

When you cannot upgrade the management group from the RMS because it does not meet the minimum supported configurations for System Center 2012 – Operations Manager, you must restore the encryption key on the Operations Manager 2007 R2 secondary manager server from which you will run the management group upgrade. For more information about whether the RMS meets the required supported configurations, see [Supported Configurations for System Center 2012 - Operations Manager](#). You should restore the encryption key just prior to upgrading the management group. To restore the encryption key, you must use the SecureStorageBackup tool.

▶ **To restore up the RMS encryption key by using the Encryption Key Backup or Restore Wizard**

1. Log on to the computer hosting the secondary management server with an account that is a member of the Administrators group.
2. Open a command prompt window by using the **Run as Administrator** option.
3. At the command prompt, type:
cd <Operations Manager Installation Folder>
SecureStorageBackup
4. In the **Encryption Key Backup or Restore Wizard**, on the **Backup or Restore?** page, select the **Restore the Encryption Key** option and then complete the wizard, providing location and password for the key.

▶ **To restore the RMS encryption key by using the command prompt**

1. Log on to the computer hosting the secondary management server with an account that is a member of the Administrators group.
2. In a Command Prompt window using the **Run as Administrator** option, type:
cd <Operations Manager Installation Folder>
SecureStorageBackup Restore <BackupFile>
3. At the **Please enter the password to use for storage/retrieval** prompt, type the password, and then press Enter.
4. Use the same password that was used to back up the encryption keys.

▶ **To verify that the RMS encryption key has been restored**

1. On the **Start** menu, click **Run**.
2. Type **regedit**, and then click **OK**. The Registry Editor starts.

 **Caution**

Incorrectly editing the registry can severely damage your system. Before you make changes to the registry, back up any valued data that is on the computer.

3. Navigate to the **HKLM\Software\microsoft\Microsoft Operations Manager\3.0\MOMBins** key. If **value1** and **value2** exist, the encryption key has successfully been restored.

Back up the Operations Manager Databases

Obtain verified recent backups of the operational database and of the data warehouse database before you upgrade the secondary management server. You should also create backups of databases for optional features, such as the Reporting and the Audit Collection Services database before you upgrade them. For more information, see [How to: Back up a Database](#) and [How to Schedule Backups of System Center 2012 - Operations Manager Databases](#).

Upgrade SQL Server Reporting Services

System Center 2012 – Operations Manager requires either SQL Server 2008 R2 or SQL Server 2008 R2 Sp1 on the SQL Server Reporting Services database (SSRS). For information about upgrading to SQL Server, see [Upgrading to SQL Server 2008 R2](#).

See Also

[Upgrade Path Checklists for Operations Manager](#)

Upgrade Tasks for Operations Manager

Upgrading an installation of System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager is a multistep process. Before you can upgrade your monitoring environment, you have to understand exactly what you are upgrading, the pre-upgrade steps, and the implications for your day-to-day operations.

Upgrade Phases

When you upgrade a single-server management group, you run the upgrade on all features installed on a single server. In a distributed management group upgrade, upgrade tasks are performed in a number of phases.

Each type of upgrade requires some pre-upgrade and post-upgrade tasks. The phases of upgrade include the following:

Upgrade phase	Description
Pre-Upgrade Tasks	<p>Pre-upgrade tasks might have to be performed before any of the upgrade phases. For more information, see Pre-Upgrade Tasks for Operations Manager.</p> <p>The starting point for an upgrade is having an Operations Manager 2007 R2 topology and ensuring that all hardware and software meets the supported configurations for System Center 2012 – Operations Manager.</p>
Secondary Management Server Upgrade	<p>In a distributed management group upgrade, you upgrade the secondary management servers (excluding the root management server), the gateways, and agents. The order of</p>

Upgrade phase	Description
	<p>agent upgrade depends on how the agents were deployed. If you installed the agents manually, you upgrade the agents before you upgrade the management servers and gateways. If you installed the agents by using the Computer and Device Management Wizard (the Discovery wizard), you upgrade the agents after you upgrade the management servers and gateways. These kinds of agents are known as push-installed agents.</p>
Management Group Upgrade	<p>In a distributed management group upgrade, the root management server (RMS), operational database, data warehouse database, and management group are upgraded. If the RMS does not meet system requirements, upgrade is run from a secondary management server.</p> <p>In a single-server management group upgrade, you upgrade manually installed agents first, and then run the management group upgrade. Push-installed agents can be upgraded after you upgrade the management group.</p>
Optional Upgrade	<p>Additional features can be upgraded, including operations consoles, web consoles, reporting server, and Audit Collection Services (ACS).</p>
Post-Upgrade Tasks	<p>Post-upgrade tasks, such as turning on notifications, must be performed after you have completed your upgrade. For more information, see Post-Upgrade Tasks when Upgrading from Operations Manager 2007 R2.</p>

Upgrading with the Exchange 2010 Management Pack

The Exchange 2010 Management Pack includes the Correlation Engine, which is usually installed on the same system as the Operations Manager RMS. For a simple upgrade, where the system supports System Center 2012 – Operations Manager, you do not have to change the Exchange 2010 Management Pack.

For a complex upgrade, where Operations Manager must be moved to a different system, do one of the following:

- Uninstall the Exchange 2010 MP from its current system using the Windows Installer package, upgrade Operations Manager to the new system, and run the Windows Installer package to install the Exchange 2010 MP on the new system. Do not remove the Exchange 2010 MP in the Operations console.
- Upgrade Operations Manager to the new system and configure the Exchange 2010 MP correlation engine to point to that system by editing Microsoft.Exchange.Monitoring.CorrelationEngine.exe.config. The default location for this file is: C:\Program Files\Microsoft\Exchange Server\v14\Bin. Change the **value** in the following line to equal the FQDN of the new Operations Manager system:

```
<add key="OpsMgrRootManagementServer" value="localhost" />
```



Note

If your Exchange 2010 MP correlation engine is installed on a cluster, you need to edit the configuration file on each member of the cluster.

See Also

[Upgrading to System Center 2012 - Operations Manager](#)

Improving Upgrade Performance

The upgrade of a management server that hosts more than 800 agents might take more than one hour. You can significantly reduce the required time to perform an upgrade by running several SQL Server commands. Use the following procedure for each management server that hosts 800 or more agents. It can also be used if the upgrade of a particular management server is taking over an hour. You can implement this procedure either before you start the upgrade or while the upgrade is running.

► To improve upgrade performance

1. On the computer that hosts the operational database, open **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, in the **Server Type** list, select **Database Engine**.
3. In the **Server Name** list, select the server and instance for your Operations Manager database (for example, computer\INSTANCE1).
4. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
5. In the **Object Explorer** pane, right-click the computer and instance name at the top of the Object Explorer tree, and then click **New Query**.
6. In the **New Query** results pane, type the following three SQL commands:

```
use OperationsManager
exec sp_updatestats
DBCC FREEPROCCACHE
```



Note

The `use` command assumes that the name of the operational database was not

changed and the default value of `OperationsManager` is used.

7. Click the **Query** menu, and then click **Execute**.
8. Click the **File** menu, and then click **Exit**.

Upgrade Helper Management Pack

The Upgrade Helper management pack guides you through the upgrade process from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager for a distributed topology. If you have a single-server management group, you can run an upgrade without the management pack. For more information, see [Upgrading a Single-Server Operations Manager 2007 R2 Environment](#).

Note

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

The Upgrade Helper management pack discovers the root management server, secondary management servers, gateway servers, and any agent-managed computers in your distributed Operations Manager 2007 R2 management group. The Upgrade Helper management pack monitors the progress of each phase of your upgrade.

Note

You might have to perform a number of pre-upgrade tasks before each phase of upgrade. For more information, see [Upgrade Path Checklists for Operations Manager](#).

Importing and Using the Upgrade Helper Management Pack

The Upgrade Helper management pack is available on the System Center 2012 – Operations Manager installation media.

Note

It may take up to 15 minutes for discovery to run after you first import the management pack.

To import the Upgrade Helper Management pack

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 R2 management group.
2. In the Operations console, click **Administration**.

Note

When you run the Operations console on a computer that is not a management

server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the management server from which you want to connect to the Operations console.

3. Right-click the **Management Packs** node, and then click **Import Management Packs**.
4. In the Import Management Packs wizard, click **Add**, and then click **Add from disk**.
5. The **Select Management Packs to import** dialog box opens. Browse to the /ManagementPacks directory of the Operations Manager installation media. Select **OperationsManager.Upgrade.mp**, and then click **Open**.
6. The **Select Management Packs** page lists the management pack that you selected for import. A green check mark next to the management pack in the list indicates that the management pack can be imported. Click **Install**.

The **Import Management Packs** page appears and shows the progress for the management pack. The management pack is downloaded to a temporary directory, imported to Operations Manager 2007 R2, and then deleted from the temporary directory. If there is a problem at any stage of the import process, select the management pack in the list to view the status details.

7. Click **Close**.

After you have imported the Upgrade Helper management pack, you can view steps for each upgrade phase in the **Monitoring** workspace of the Operations console.

Important

Typically, you follow each of the steps in the Upgrade Helper management pack in order. However, if you have manually installed agents, you should upgrade them before you upgrade the secondary management servers. You upgrade push-installed agents after you upgrade the secondary management servers.

To review the status of the secondary management servers in your management group

1. In the Operations Manager 2007 R2 console, in the navigation pane, click the **Monitoring** button.
2. Expand **Operations Manager 2007 R2 -> 2012 Upgrade MP**, and then click **Step 1: Upgrade Secondary Management Servers**. This displays all secondary management servers in your management group.
3. Review the state of each management server. If the secondary management server is upgraded, the state is **Healthy**. If it is not upgraded, a **Warning** appears.
4. You must upgrade each secondary management server and ensure that the status is healthy before you move to the next step in the process. For more information, see [How to Upgrade a Secondary Management Server from Operations Manager 2007 R2](#).

Note

You can open the discovered instances with the Operations Manager Health Explorer to see the upgrade status, with additional information about how to upgrade the management servers.

▶ **To review the status of the gateway servers in your management group**

1. In the Operations Manager 2007 R2 console, in the navigation pane, click the **Monitoring** button.
2. Expand **Operations Manager 2007 R2 -> 2012 Upgrade MP**, and then click **Step 2: Upgrade Gateway Servers**. This displays all gateway servers in your management group.
3. Review the state of each gateway server. If the gateway server is upgraded, the state is **Healthy**. If it is not upgraded, a **Warning** appears.
4. You must upgrade each gateway server and ensure that the status is healthy before you move to the next step in the process. For more information, see [How to Upgrade a Gateway Server from Operations Manager 2007 R2](#).



Note

You can open the discovered instances with the Health Explorer to see the upgrade status, with additional information about how to upgrade the gateways.

▶ **To review the status of the agents in your management group**

1. In the Operations Manager 2007 R2 console, in the navigation pane, click the **Monitoring** button.
2. Expand **Operations Manager 2007 R2 -> 2012 Upgrade MP**, and then click **Step 3: Upgrade Agents**. This displays all agent-managed computers in your management group. It also displays additional properties about the agents, such as **IsManuallyInstalled** and **DeployedViaActiveDirectory** to help you determine which upgrade process to follow.



Important

You must upgrade the agents that have a value of **True** in the **IsManuallyInstalled** property before you upgrade your secondary management servers.

3. Review the state of each agent. If the agent is upgraded, the state is **Healthy**. If it is not upgraded, a **Warning** appears.
4. You must upgrade the agents and ensure that the status of each is healthy before you move to the next step in the process. For more information, see [How to Upgrade Agents from Operations Manager 2007 R2](#).



Note

You can open the discovered instances with the Health Explorer to see the upgrade status, with additional information about how to upgrade the agents.

▶ **To review the status of the RMS in the management group**

1. In the Operations Manager 2007 R2 console, in the navigation pane, click the **Monitoring** button.

2. Expand **Operations Manager 2007 R2 -> 2012 Upgrade MP**, and then click **Step 4: Upgrade Management Group (RMS, DB, DW)**. This displays the root management server (RMS) in your management group.

After the secondary management servers, gateways, and agents have been upgraded, you can upgrade the management group from the RMS. This upgrade process upgrades the operational database and the data warehouse. If the data warehouse does not already exist, it is installed.

3. If the management group has been upgraded, the state is **Healthy**. If it is not upgraded, a **Warning** appears.
4. If the root management server meets the minimum supported configurations for System Center 2012 – Operations Manager, you can upgrade from the RMS. For more information, see [How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS](#). If the root management server does not meet the minimum supported configurations, you must upgrade the management group from a secondary management server. For more information, see [How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server](#). For more information about the supported configuration requirements for System Center 2012 – Operations Manager, see [Supported Configurations for System Center 2012 - Operations Manager](#).



Note

You can open the discovered instances with the Health Explorer to see the upgrade status, with additional information about how to upgrade the management group.

See Also

[Checklist: Distributed Upgrade \(Simple\)](#)

[Checklist: Distributed Upgrade \(Complex\)](#)

Upgrading Hardware and Software to Meet System Requirements

Upgrading to System Center 2012 – Operations Manager requires that you start with an System Center Operations Manager 2007 R2 management group. If you are using an earlier version of Operations Manager, you must first upgrade to Operations Manager 2007 R2. For more information, see [Operations Manager 2007 Upgrade Guide](#).

Before you begin the upgrade process to System Center 2012 – Operations Manager, you should ensure that all servers in the management group meet the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#).

If your servers do not meet the supported configuration requirements because they cannot support a 64-bit operating system, you have to add new servers that meet these requirements in addition to ensuring that all other required configuration requirements are met. The following topics describe how to perform the tasks necessary to introduce new hardware to the Operations Manager 2007 R2 management group:

- [How to Add an Operations Manager 2007 R2 Secondary Management Server \(Operations Manager Upgrade\)](#)
- [How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server \(Operations Manager Upgrade\)](#)
- [How to Replace an Operations Manager 2007 R2 Gateway that Has an Unsupported Configuration \(Operations Manager Upgrade\)](#)
- [How to Remove an Operations Manager 2007 R2 Gateway \(Operations Manager Upgrade\)](#)
- [Upgrading SQL Server \(Operations Manager Upgrade\)](#)

How to Add an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)

When you want to upgrade to System Center 2012 – Operations Manager but have a management server in your System Center Operations Manager 2007 R2 environment that does not meet the minimum supported configurations for System Center 2012 – Operations Manager, you must add a new server to replace the old one. You should install an Operations Manager 2007 R2 secondary management server, and then join it to your existing management group. Afterwards, you can move the agents from the old server to the new server. For more information, see [How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server \(Operations Manager Upgrade\)](#).

To ensure that your new server hardware and software meet the minimum supported configurations for System Center 2012 – Operations Manager, see [Supported Configurations for System Center 2012 - Operations Manager](#).

► To install a secondary management server

1. On a server that meets the supported configuration requirements for System Center 2012 – Operations Manager, install Operations Manager 2007 R2 by using the instructions in [Deploying Stand-Alone Management Servers on Windows Server 2008](#).



Note

It can take up to five minutes for the System Center Management Service on the new management server to establish secure communications with the root management (RMS) server, and during that time it appears as not monitored.

When communications are established, its Health state changes to Healthy.

The next step is to move the agents that reported to the old management server or RMS to the new secondary management server. For more information, see [How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server \(Operations Manager Upgrade\)](#).

See Also

[Upgrading Hardware and Software to Meet System Requirements](#)

How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server (Operations Manager Upgrade)

After you have added a secondary management server to your System Center Operations Manager 2007 R2 management group, you must move the agents that are reporting to the root management server (RMS) or management server that you are replacing to the new secondary management server.

You also move the agents to a secondary management server to avoid downtime when you upgrade a distributed management group that meets the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#).

Important

If you have a distributed management group that meets the minimum supported configurations, you can alternatively upgrade the agents after you upgrade the management group instead of moving the agents to a secondary management server.

However, you will experience monitoring downtime until the agents are upgraded.

You can move the agents by using the Operations console, by using Active Directory Integration, or by running a Windows PowerShell script. However, if the agents were deployed manually, you cannot move them by using the Operations console.

Moving Agents to a Secondary Management Server

To move Windows, UNIX, and Linux push-installed agents to a secondary management server by using the Operations console

1. Log on to a computer that hosts an Operations console with an Operations Manager Administrators role account for the Operations Manager 2007 R2 management group.
2. In the Operations console, click the **Administration** button.

Note

When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager 2007 R2 management server that you want the Operations console to connect to.

3. In the **Administration** pane, under **Device Management**, click **Agent-Managed**.
4. For Windows agents, right-click the computers in the **Agent-Managed** pane that have agents that you want to move to the secondary management server, and then click **Change Primary Management Server**.
For UNIX and Linux agents, right-click the computers in the **UNIX/Linux Servers** pane that have agents that you want to move to the secondary management server, and then click **Change Primary Management Server**.
5. In the **Change Management Server** dialog box, select the secondary management server from the list, and then click **OK**. The change takes effect on the agent after its next update interval.

▶ **To move Windows agents to a secondary management server by using a Windows PowerShell script**

1. Log on to a computer that hosts an Operations console with an Operations Manager Administrators role account for the Operations Manager 2007 R2 management group.
2. Run the following script.

```
$newMS = Get-ManagementServer | where {$_.Name -eq
'<SecondaryMgmtServer.DomainName.COM>'}
$agent = Get-Agent | where {$_.PrincipalName -eq
'<AgentComputer.Domain.COM>'}
Set-ManagementServer -AgentManagedComputer: $agent -
PrimaryManagementServer: $newMS
```

The Operations console should now list the secondary management server as the primary management server for the agent that was moved.

Moving Agents to a Secondary Management Server by using Active Directory Integration

Using Active Directory Integration to move Windows agents to a secondary management server is a multistep process. First, you delete the configuration rule for the management server that you will replace. Then, you create a new rule that sets the replacement management server as the failover management server. This step is an intermediary step that is required for the agent to recognize the replacement management server. After the agent assignment propagates in Active Directory Domain Services, which can take up to one hour, you delete the configuration rule that you just created. Finally, you create a new configuration rule on the replacement management server.

In the following procedures, it is assumed that you have an existing primary management server and a failover management server that do not meet the minimum configuration requirements for System Center 2012 – Operations Manager, and you have already created two new secondary management servers that do meet these requirements to replace the old ones. By creating the configuration rules for Active Directory Integration, you move the agents from the old servers to the new servers in a multistep process.

▶ **To create a configuration rule for the management server that you are replacing (step 1)**

1. Log on to a computer that hosts an Operations console with an Operations Manager Administrators role account for the Operations Manager 2007 R2 management group.
2. In the Operations console, click the **Administration** button.

 **Note**

When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager 2007 R2 management server that you want the Operations console to connect to.

3. In the **Administration** pane, under **Device Management**, click **Management Servers**.
4. In the **Management Servers** pane, right-click the management server that you are replacing, and then click **Properties**. This sets the management server that you are replacing as the **Primary Management Server** for the computers that are returned by the rules you will create in the following procedure.
5. In the **Management Server Properties** dialog box, click the **Auto Agent Assignment** tab.
6. Select the agent assignment, and then click **Delete**.

Click **Add** to start the **Agent Assignment and Failover Wizard**, and then click **Next**.



Note

The **Introduction** page does not appear if the wizard has been run and **Do not show this page again** was selected.

7. On the **Domain** page, do the following:
 - Select the domain of the computers from the **Domain name** list. The management server must be able to resolve the domain name.



Important

The management server and the computers that you want to manage must be in 2-way trusted domains.

- Select the **Use a different account to perform agent assigned in the specified domain** check box.
 - Set **Select Run As Profile** to the Run As profile associated with the Run As account that was provided when MOMADAdmin.exe was run for the domain. The default account that is used to perform agent assignment is the computer account for the root management server, also referred to as the **Active Directory-Based Agent Assignment Account**. If this was not the account that was used to run MOMADAdmin.exe, select **Use a different account to perform agent assignment in the specified domain**, and then select or create the account from the **Select Run As Profile** list.
8. On the **Inclusion Criteria** page, either type the LDAP query for assigning computers to this management server, and then click **Next**, or click **Configure**. If you click **Configure**, do the following:
 - a. In the **Find Computers** dialog box, type the criteria that you want to use for assigning computers to this management server.
 - b. Click **OK**, and then click **Next**.



Note

The following LDAP query returns computers with a name starting with MsgOps, **(&(sAMAccountType=805306369)(objectCategory=computer)(cn=MsgOps*))**
For more information about LDAP queries, see [Creating a Query Filter](#).

9. On the **Exclusion Rule** page, type the fully qualified domain name (FQDN) of computers that you explicitly want to prevent from being managed by this management server, and then click **Next**.

 **Important**

You must separate the computer FQDNs that you type with a semicolon, colon, or a new line (CTRL+ENTER).

10. On the **Agent Failover** page, select **Manually configure failover**, and then do the following:
 - a. Select the check box of the replacement secondary management server. This sets the replacement server as the failover server.
 - b. Click **Create**.
11. In the **Management Server Properties** dialog box, click **OK**.

 **Note**

It can take up to one hour for the agent assignment setting to propagate in Active Directory Domain Services.

12. After you have confirmed that the agent assignment was successful, delete the agent assignment that you created earlier.

 **To create a configuration rule for the replacement management server (step 2)**

1. In the Operations console, click the **Administration** button.
2. In the **Administration** pane, under **Device Management**, click **Management Servers**.
3. In the **Management Servers** pane, right-click the replacement secondary management server, and then click **Properties**. This sets the replacement management server as the **Primary Management Server** for the computers that are returned by the rules that you will create in the following procedure.
4. In the **Management Server Properties** dialog box, click the **Auto Agent Assignment** tab.
5. Click **Add** to start the **Agent Assignment and Failover Wizard**, and then click **Next**.

 **Note**

The **Introduction** page does not appear if the wizard has been run and **Do not show this page again** was selected.

6. On the **Domain** page, do the following:
 - Select the domain of the computers from the **Domain name** list. The management server must be able to resolve the domain name.

 **Important**

The management server and the computers that you want to manage must be in 2-way trusted domains.

- Select the **Use a different account to perform agent assigned in the specified domain** check box.
- Set **Select Run As Profile** to the Run As profile associated with the Run As account that was provided when MOMADAdmin.exe was run for the domain. The default account that is used to perform agent assignment is the computer account for the

root management server, also referred to as the **Active Directory-Based Agent Assignment Account**. If this was not the account that was used to run MOMADAdmin.exe, select **Use a different account to perform agent assignment in the specified domain**, and then select or create the account from the **Select Run As Profile** list.

7. On the **Inclusion Criteria** page, either type the LDAP query for assigning computers to this management server, and then click **Next**, or click **Configure**. If you click **Configure**, do the following:
 - a. In the **Find Computers** dialog box, type the criteria that you want to use for assigning computers to this management server.
 - b. Click **OK**, and then click **Next**.



Note

The following LDAP query returns computers with a name starting with MsgOps, **(&(sAMAccountType=805306369)(objectCategory=computer)(cn=MsgOps*))**
For more information about LDAP queries, see [Creating a Query Filter](#).

8. On the **Exclusion Rule** page, type the fully qualified domain name (FQDN) of computers that you explicitly want to prevent from being managed by this management server, and then click **Next**.



Important

You must separate the computer FQDNs that you type with a semicolon, colon, or a new line (CTRL+ENTER).

9. On the **Agent Failover** page, select **Manually configure failover**, and then do the following:
 - a. Select the check box of the second replacement management server that you added to the management group. This sets it as the failover server.
 - b. Click **Create**.
10. In the **Management Server Properties** dialog box, click **OK**.



Note

It can take up to one hour for the agent assignment setting to propagate in Active Directory Domain Services.

See Also

[Upgrading Hardware and Software to Meet System Requirements](#)

How to Replace an Operations Manager 2007 R2 Gateway that Has an Unsupported Configuration (Operations Manager Upgrade)

If you have an System Center Operations Manager 2007 R2 gateway server that does not meet the minimum supported configuration requirements for System Center 2012 – Operations Manager, you must replace the gateway server before you upgrade to System Center 2012 – Operations Manager. For more information, see [Supported Configurations for](#)

[System Center 2012 - Operations Manager](#). This procedure shows you how to add a new Operations Manager 2007 R2 gateway and to prepare it for upgrade.

Replacing an Operations Manager 2007 R2 Gateway Server

The steps you take to replace the gateway server include the following:

1. Register the computer that will host the gateway with the management group. See [Registering the Gateway with the Management Group](#).
2. Install the Operations Manager 2007 R2 gateway server. See [Installing a Gateway Server](#).
3. Deploy and import certificates on the gateway and management servers. See [Deploying the Certificates](#).
4. Remove the old gateway server. See [How to Remove an Operations Manager 2007 R2 Gateway \(Operations Manager Upgrade\)](#).

Registering the Gateway with the Management Group

Before you install a new Operations Manager 2007 R2 gateway server, you must register the computer that will host the gateway with the management group. This procedure registers the gateway server with the management group, and when registration is completed, the gateway server appears in the **Discovered Inventory** view of the management group.

You must first copy the gateway approval tool

(Microsoft.EnterpriseManagement.GatewayApprovalTool.exe) to the management server. This tool is required only on the management server, and it only has to be run one time.

▶ To copy Microsoft.EnterpriseManagement.GatewayApprovalTool.exe to management servers

1. From a targeted management server, open the Operations Manager 2007 R2 installation media \SupportTools directory.
2. Copy the Microsoft.EnterpriseManagement.GatewayApprovalTool.exe from the installation media to the targeted management server. You should copy it to the installation directory of the management server.

▶ To run the gateway approval tool

1. Log on to the management server that the gateway server will target by using the Operations Manager Administrators credentials.
2. Open a Command Prompt window, and browse to the directory where you copied Microsoft.EnterpriseManagement.gatewayApprovalTool.exe.
3. At the command prompt, run
Microsoft.EnterpriseManagement.gatewayApprovalTool.exe /ManagementServerName=<managementserverFQDN> /GatewayName=<GatewayFQDN> /Action=Create
4. If the approval is successful, the following message appears **The approval of server <GatewayFQDN> completed successfully.**
5. Open the Operations console to the Monitoring view. Select the Discovered Inventory view to verify that the gateway server is present.

Installing a Gateway Server

You must install an Operations Manager 2007 R2 gateway on a server that meets the minimum supported configuration requirements for System Center 2012 – Operations Manager.

► To install an Operations Manager 2007 R2 gateway server

1. Log on to the gateway server with local administrator rights.
2. From the Operations Manager 2007 R2 installation media, run **SetupOM.exe**.
3. In the **Install** area, click the **Install Operations Manager 2007 R2 Gateway** link.
4. On the **Welcome** page, click **Next**.
5. On the **Destination Folder** page, accept the default, or click **Change** to select a different installation directory, and then click **Next**.
6. On the **Management Group Configuration** page, type the targeted management group name in the **Management Group Name** box, type the targeted management server name in the **Management Server** box, check that the **Management Server Port** box is **5723**, and then click **Next**. This port can be changed if you have enabled a different port for management server communication in the Operations console.
7. On the **Gateway Action Account** page, select the **Local System** account option, unless you have specifically created a domain-based or local computer-based gateway action account. Click **Next**.
8. On the **Microsoft Update** page, optionally indicate if you want to use Microsoft Update, and then click **Next**.
9. On the **Ready to Install** page, click **Install**.
10. On the **Completing Installation** page, click **Finish**.

Deploying the Certificates

Because the gateway server is not trusted by the domain that the management group is in, certificates must be used to establish the identity of each gateway server and management server. This arrangement satisfies the requirement of Operations Manager for mutual authentication. You must request and download the certificates, and then import them by using the Operations Manager 2007 R2 MOMCertImport.exe tool.

Reliable name resolution must exist between the agent-managed computers and the gateway server and between the gateway server and the management servers. Typically, Domain Name System (DNS) is used to resolve host names, such as www.contoso.com, to their corresponding IP addresses. However, if it is not possible to get proper name resolution through DNS, you might have to manually create entries in the Hosts file of each computer to resolve host names to IP addresses.



Note

The Hosts file is located in a subdirectory of the C:\Windows\System32\Drivers, and it contains directions for configuration.

After you have downloaded the certificates to each gateway server and management server, you import them by using the MOMCertImport tool.

▶ **To request and download certificates**

1. Request and download a Trusted Root (CA) certificate on each gateway and management server.

▶ **To import computer certificates by using MOMCertImport.exe**

1. Copy the MOMCertImport.exe tool from the installation media \SupportTools directory to the root of the gateway server or to the Operations Manager 2007 R2 installation directory of the management server.
2. Open a Command Prompt window by using the **Run as Administrator** option, change to the directory to the location of MOMCertImport.exe, and then run **momcertimport.exe /SubjectName <certificate subject name>**. This makes the certificate usable by Operations Manager.



Tip

If you double-click MOMCertImport.exe or run it at the Command Prompt window without any parameters, a dialog box appears where you can select the installed certificate, and then click **OK**.

The next step is to remove the old gateway server from the management group. For more information, see [How to Remove an Operations Manager 2007 R2 Gateway \(Operations Manager Upgrade\)](#).

See Also

[Upgrading Hardware and Software to Meet System Requirements](#)

[How to Remove an Operations Manager 2007 R2 Gateway \(Operations Manager Upgrade\)](#)

How to Remove an Operations Manager 2007 R2 Gateway (Operations Manager Upgrade)

After you have replaced a System Center Operations Manager 2007 R2 gateway server that does not meet the minimum supported configurations for System Center 2012 – Operations Manager, you can remove the old gateways from the management group and uninstall the old gateway from the server. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

You must first copy the gateway approval tool (Microsoft.EnterpriseManagement.GatewayApprovalTool.exe) from the \SupportTools directory of the Operations Manager 2007 R2 installation media to the management server, if it does not already exist.

▶ **To uninstall the gateway server**

1. Log on to the gateway server to be removed with the Operations Manager 2007 R2 Administrators credentials.
2. In Control Panel, in **Programs and Features**, right-click **System Center Operations Manager 2007 R2 Gateway**, and then click **Uninstall**.

► **To remove a gateway from the management group**

1. On the management server that was targeted during the gateway server installation, log on with Operations Manager Administrators credentials.
2. Open a Command Prompt window, and browse to the directory to where you copied Microsoft.EnterpriseManagement.gatewayApprovalTool.exe.
3. At the command prompt, run the following command, where GatewayName is the name of the gateway that you want to remove.
Microsoft.EnterpriseManagement.gatewayApprovalTool.exe /ManagementServerName=<managementserverFQDN> /GatewayName=<GatewayFQDN> /Action=Delete
4. Open the Operations console to the Monitoring view. Select the **Discovered Inventory** view to see that the gateway server is no longer present.

See Also

[Upgrading Hardware and Software to Meet System Requirements](#)

Upgrading SQL Server (Operations Manager Upgrade)

Upgrading to System Center 2012 – Operations Manager requires Microsoft SQL Server 2008 SP1, SQL Server 2008 R2, or SQL Server 2008 R2 SP1 for the operational database, data warehouse database, and Audit Collection Services (ACS) database. If your servers do not support this upgrade, you have to add new servers and move your SQL Server databases from the old servers to the new servers. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#).

For more information about how to move your System Center Operations Manager 2007 R2 databases, see:

- [How to Move the Operational Database](#)
- [How to Move the Data Warehouse Database](#)
- [How to Move the OperationsManagerAC Database in Operations Manager 2007](#)

For more information about how to upgrade a database, see:

- [How to: Upgrade to SQL Server 2008 R2 \(Setup\)](#)
- [Upgrading to SQL Server 2008 R2](#)

Upgrading a Single-Server Operations Manager 2007 R2 Environment

When you upgrade a single-server System Center Operations Manager 2007 R2 environment to System Center 2012 – Operations Manager, you run the upgrade on all features on a single server. If a data warehouse does not already exist, it is created during the upgrade process because having a data warehouse is a requirement for System Center 2012 – Operations Manager. You upgrade any manually installed agents before you run upgrade on the management group. If you installed agents by using the **Computer and Device Management Wizard** (the Discovery wizard), you can upgrade these agents after you upgrade the management group by using the Operations Manager Operations console.

The following topics describe how to perform the necessary steps to upgrade a single-server management group that has a supported configuration for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#).

- [How to Upgrade an Operations Manager 2007 R2 Single-Server Management Group](#)
- [Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group](#)

See Also

[Checklist: Single-Server Upgrade \(Simple\)](#)

[Checklist: Single-Server Upgrade \(Complex\)](#)

[Single-Server and Distributed Upgrade Process Flow Diagram](#)

How to Upgrade an Operations Manager 2007 R2 Single-Server Management Group

When you upgrade a System Center Operations Manager 2007 R2 single-server management group to System Center 2012 – Operations Manager, all features that are installed on the server are upgraded. This includes the Operations Manager 2007 R2 operational database, management server, operations console, web console, and Reporting server, if installed. The Operations Manager 2007 R2 data warehouse is also upgraded, if it exists. Otherwise, the **System Center Operations Manager 2012 Setup Wizard** installs it.

Important

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

If your single-server management group meets the supported configuration requirements, but you do not want to experience any downtime during the upgrade process, you can add a secondary management server, and then follow the upgrade process for a distributed upgrade. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#). If your server cannot meet the supported configurations because it requires new hardware, you can add a secondary management server, and then follow the upgrade process for a distributed upgrade. For more information, see [Upgrade Path Checklists for Operations Manager](#).

To upgrade a single-server management group

1. Log on to the computer that is hosting a root management server (RMS) with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer.
2. On the System Center 2012 – Operations Manager media, run **Setup.exe**, and then click **Install**.

**Note**

The **Getting Started** page displays information about what will be upgraded. The Operations Manager data warehouse will be installed if it does not already exist.

Click **Next** to proceed with the upgrade.

3. On the **Getting Started, Please read the license terms** page, read the Microsoft Software License Terms, click **I have read, understood, and agree with the license terms**, and then click **Next**.
4. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.

**Note**

Microsoft SQL Server Full Text Search must be enabled.

**Note**

The **Agent Upgrade Check** warning can be ignored if you plan to upgrade the agents after the single-server management group has been upgraded.

6. If the Prerequisites checker does not return any other errors or warnings that have to be addressed, click **Next**.
7. If the single-server management group does not already have a data warehouse installed, a data warehouse is created, and you must configure it as follows:
 - a. On the **Configure the data warehouse database** page, in the **Server name and instance name** box, type the server name of the SQL Server database and instance for the database server that will host the data warehouse database.
 - b. After you have typed in the correct values for the server name of the SQL Server database, Setup attempts to validate the values that you have typed as the SQL Server name and the port number. In the **Database name**, **Database size (MB)**, **Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.

**Warning**

These paths do not change if you connect to a different instance of SQL Server.

- c. On the **Configuration, Specify a web site for use with the Web console** page, select the **Default Web Site**, or the name of an existing website. Select **Enable SSL** only if the website has been configured to use Secure Sockets Layer (SSL), and then click **Next**.
 - d. On the **Configuration, Select an authentication mode for use with the Web console** page, select your options, and then click **Next**.
8. On the **Configuration, Configure Operations Manager accounts** page, we recommend that you use the **Domain Account** option for the **System Center**

Configuration service and System Center Data Access service accounts. Enter the credentials for a domain account in each box, and then click **Next**.

 **Important**

If you receive a message about using the wrong version of SQL Server, or experience a problem with the SQL Server Windows Management Instrumentation (WMI) provider, you can resolve this. Open a Command Prompt window by using the **Run as administrator** option. Then run the following command, where <path> is the location of Microsoft SQL Server:

```
mofcomp.exe "<path>\Microsoft SQL  
Server\100\Shared\sqlmgmproviderxpsp2up.mof".
```

9. When the **Ready to Upgrade** page appears, review the upgrade summary, and then click **Upgrade**.

 **To upgrade a single-server management group by using the Command Prompt window**

1. Log on to the computer that is hosting a RMS with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the System Center 2012 – Operations Manager Setup.exe file is located.

 **Important**

Use the `/WebConsoleUseSSL` parameter only if your website has Secure Sockets Layer (SSL) activated. For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.

 **Note**

If the web console reports to an unsupported or inaccessible root management server, you must also pass the following parameter:

```
/ManagementServer:<servername>.
```

 **Important**

The following commands assume that you specified the Local System for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead:

```
/DASAccountUser: <domain\username> /DASAccountPassword: <password>
```

If you installed a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

```
setup.exe /silent /upgrade /UseLocalSystemDASAccount  
/WebsiteName: "<WebSiteName>" [/WebConsoleUseSSL]  
/WebConsoleAuthorizationMode: [Mixed|Network]
```

If you did not install a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

```
Setup.exe /silent /upgrade /UseLocalSystemDASAccount  
/AcceptEndUserLicenseAgreement  
/WebsiteName: "<WebSiteName>" [/WebConsoleUseSSL]  
/WebConsoleAuthorizationMode: [Mixed|Network]  
/DWSqlServerInstance: <server\instance>  
/DWDatabaseName: <DW name>  
/DataReaderUser: <domain\username>  
/DataReaderPassword: <password>  
/DataWriterUser: <domain\username>  
/DataWriterPassword: <password>
```

See Also

[Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group](#)

[Checklist: Single-Server Upgrade \(Simple\)](#)

[Checklist: Single-Server Upgrade \(Complex\)](#)

Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group

You can upgrade System Center Operations Manager 2007 R2 agents in a single-server management group by using the Operations console, manually by using the Setup Wizard, or manually, by using a command prompt. Determining which option to use depends on how the agents were deployed. For example, agents that were installed by using the **Computer and Device Management Wizard** (“push-installed agents”) can be upgraded through the Operations console. However, agents that were installed manually (“manually installed agents”) cannot be upgraded this way. You can verify how agents were installed by using the Upgrade Helper management pack. For more information, see [Upgrade Helper Management Pack](#).

Important

For information about how upgrade works with AVIcode 5.7 agents and .NET Application Performance Monitoring Agents, see [Notes for AVIcode 5.7 Customers](#).

You should upgrade manually installed agents before you run upgrade on the management group. Push-installed agents can be upgraded after you run upgrade on the management group. You use the System Center 2012 – Operations Manager Operations console to upgrade push-installed agents in a single-server management group.

For information about how to upgrade Windows agents and UNIX and Linux agents, see [How to Upgrade Agents from Operations Manager 2007 R2](#).

See Also

[Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group](#)

Upgrading a Distributed Operations Manager 2007 R2 Environment

When you upgrade a distributed System Center Operations Manager 2007 R2 environment to System Center 2012 – Operations Manager, you start by upgrading any manually installed agents, followed by the secondary management servers, gateways, and any push-installed agents. You then run upgrade of the management server either on the root management server (RMS), if it meets the minimum supported configurations for Operations Manager, or from the secondary management server if it does not meet these requirements. You can then upgrade additional, optional features, such as consoles, the Reporting server, and the Audit Collection Services (ACS) Collector.

Important

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

The following topics describe how to perform the necessary steps in a distributed management group upgrade. The specific upgrade path you take depends on your current environment. For information on choosing an upgrade path, see [Upgrade Path Checklists for Operations Manager](#).

- [How to Upgrade a Secondary Management Server from Operations Manager 2007 R2](#)
- [How to Upgrade a Gateway Server from Operations Manager 2007 R2](#)
- [Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group](#)
- [How to Upgrade Agents from Operations Manager 2007 R2](#)
- [How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS](#)
- [How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server](#)
- [How to Upgrade a Stand-Alone Operations Console from Operations Manager 2007 R2](#)
- [How to Upgrade a Web Console from Operations Manager 2007 R2](#)
- [How to Upgrade Reporting from Operations Manager 2007 R2](#)
- [How to Upgrade an ACS Collector from Operations Manager 2007 R2](#)

See Also

[Checklist: Distributed Upgrade \(Simple\)](#)

[Checklist: Distributed Upgrade \(Complex\)](#)

[Distributed Upgrade \(Complex\) Process Flow Diagram](#)

[Single-Server and Distributed Upgrade \(Simple\) Process Flow Diagram](#)

[Upgrading a Single-Server Operations Manager 2007 R2 Environment](#)

How to Upgrade a Secondary Management Server from Operations Manager 2007 R2

This procedure demonstrates how to upgrade a System Center Operations Manager 2007 R2 secondary management server to System Center 2012 – Operations Manager in a distributed environment. To learn more about each upgrade path and the order in which to perform each upgrade task, see the [Upgrade Path Checklists for Operations Manager](#).

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

► To upgrade a secondary management server

1. Log on to the secondary management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer.
2. From the System Center 2012 – Operations Manager media, run **Setup.exe**, and then click **Install**. The **Getting Started** page displays information about which features will be upgraded.

Note

If a web console exists on the secondary management server, it will be removed instead of upgraded. You have to re-install the web console after you upgrade the management group. For more information, see [How to Install the Operations Manager Web Console](#). To minimize downtime, you can install the Operations Manager 2007 R2 web console on a stand-alone server.

3. On the **Getting Started, System Center 2012 - Operations Manager Upgrade** page, click **Next** to proceed with the upgrade.
4. On the **Getting Started, Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location, or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration, Configure Operations Manager accounts** page, we recommend that you use the **Domain Account** option for the **System Center Configuration service and System Center Data Access service** accounts. Enter the credentials for a domain account, and then click **Next**.
8. Review the options on the **Configuration, Ready To Upgrade** page, and then click **Upgrade**. The upgrade proceeds and displays the upgrade progress.
9. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

Upgrading a secondary management server is just one phase of the distributed upgrade process. Upgrade is not completed until you have upgraded all of the other features in your management group, and have run upgrade on the management group itself. The next step is to upgrade any gateways.

► **To upgrade a secondary management server by using the Command Prompt window**

1. Log on to the secondary management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the System Center 2012 – Operations Manager setup.exe file is located, and run the following command.



Important

The following commands assume that you specified the Local System account for the Data Access service (/UseLocalSystemDASAccount). To specify a domain\user name for these accounts, you must provide the following parameters instead.

```
/DASAccountUser: <domain\username> /DASAccountPassword: <password>  
  
setup.exe /silent /upgrade  
  
/UseLocalSystemDASAccount  
  
/DataReaderUser:<domain\user>  
  
/DataReaderPassword:<domain\user>
```

See Also

[How to Upgrade a Gateway Server from Operations Manager 2007 R2](#)

[How to Upgrade Agents from Operations Manager 2007 R2](#)

[Upgrading a Distributed Operations Manager 2007 R2 Environment](#)

[Upgrade Path Checklists for Operations Manager](#)

How to Upgrade a Gateway Server from Operations Manager 2007 R2

After you upgrade the secondary management server, you upgrade any gateway servers. The procedure to upgrade a gateway server from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager is performed locally on the gateway server. You can then verify whether the upgrade is successful.

For more information about each upgrade path and the order in which to perform each upgrade task, see the [Upgrade Path Checklists for Operations Manager](#).

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to

add any new servers to your management group before you upgrade. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

▶ **To upgrade a gateway server**

1. Log on to a computer that hosts the gateway server with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. On the System Center 2012 – Operations Manager media, run **Setup.exe**.
3. In the **Optional Installations** area, click **Gateway management server**.
4. On the **Welcome to the System Center 2012 - Operations Manager Gateway Upgrade Wizard** page, click **Next**.
5. On the **The wizard is ready to begin gateway upgrade** page, click **Upgrade**.
6. On the **Completing the System Center 2012 - Operations Manager Gateway Setup wizard** page, click **Finish**.

▶ **To upgrade a gateway server by using the Command Prompt window**

1. Log on to a computer that is hosting the gateway server with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the directory to the System Center 2012 – Operations Manager installation media and change directory again to gateway\AMD64, where the MOMGateway.msi file is located.
4. Run the following command where D:\ is the location for the upgrade log file.

```
msiexec /i MOMgateway.msi /qn /l*v D:\logs\GatewayUpgrade.log
```

▶ **To verify the gateway server upgrade**

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **Management Servers**.
3. In the **Management Servers** pane, verify that the value listed in the **Version** column is 7.0.85xx.x, where x is any positive integer.

See Also

[Upgrading a Distributed Operations Manager 2007 R2 Environment](#)

[Upgrade Path Checklists for Operations Manager](#)

Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group

You can upgrade System Center Operations Manager 2007 R2 agents in a distributed management group by using the Operations console, or manually, by using the Setup Wizard or by using a command prompt. Determining which option to use depends on how the agents were deployed. For example, you can upgrade agents that were installed by using the Computer and Device Management Wizard (“push-installed agents”) through the Operations console. However, agents that were installed manually (“manually installed agents”) cannot be upgraded this way.

You can use the Upgrade Helper management pack to verify how agents were installed. For more information, see [Upgrade Helper Management Pack](#).

 **Important**

For information about how upgrade works with AVIcode 5.7 agents and .NET Application Performance Monitoring Agents, see [Notes for AVIcode 5.7 Customers](#).

You should upgrade manually installed agents before you run upgrade on the secondary management server. Push-installed agents can be upgraded after you run upgrade on the secondary management server, before you upgrade the management group. You use the Operations Manager 2007 R2 Operations console to upgrade push-installed agents in a distributed topology.

When you move the push-installed agents to a secondary management server by using the Operations console, they are placed in Pending Management, and you must approve the update to upgrade the agents to System Center 2012 – Operations Manager.

For information about how to upgrade agents, see [How to Upgrade Agents from Operations Manager 2007 R2](#)

See Also

[Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group](#)

[Upgrading a Distributed Operations Manager 2007 R2 Environment](#)

[Upgrade Path Checklists for Operations Manager](#)

How to Upgrade Agents from Operations Manager 2007 R2

The order in which you upgrade agents depends on how they were installed and whether you are upgrading a single-server management group or a distributed management group. For more information, see [Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group](#) and [Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group](#).

When you upgrade an agent, the System Center 2012 – Operations Manager installer service runs and is not removed until after the completion of the upgrade. If the agent upgrade fails, you might have to re-install the agent, because the installer service was not properly removed. If you attempt to upgrade the agent again and it fails, you should re-install the agent after you have completed upgrading all features of Operations Manager.

Use the following procedures to upgrade System Center Operations Manager 2007 R2 agents to System Center 2012 – Operations Manager agents. If you are upgrading agents that are deployed to a computer that has other Operations Manager 2007 R2 features installed, you must take the following steps:

- If the agent is installed on a computer that has the Operations Manager 2007 R2 Operations console or web console installed, you must first uninstall the consoles before you upgrade the agents. You can do this by uninstalling **System Center Operations Manager 2007** in **Programs and Features**. You can reinstall these consoles after upgrade is completed.
- If the agent is installed on computer that has an Operations Manager 2007 R2 operational database and at least one Reporting feature (such as the data warehouse server or

Reporting server), uninstall **System Center Operations Manager 2007** in **Programs and Features**. Do not uninstall **System Center Operations Manager 2007 Reporting**.

- If the agent is installed on a computer that is an Operations Manager 2007 R2 secondary management server, you should remove the agents from the management server. After management group upgrade is completed, you should run repair on that management server.

If you have ACS installed, after the agent upgrade is complete, you must manually start the ACS forwarding service and change the startup setting to automatic.

After you upgrade the server hosting ACS and any agents that act as ACS forwarders, you may need to re-enable ACS forwarding on the agents. In Operations console, go to the **Monitoring** workspace and in the navigation pane, select **Microsoft Audit Collection Services**, then expand **Forwarder**, then expand **State View**. If any of your forwarders do not appear, re-enable them. For more information, see **How to Enable Audit Collection Services (ACS) Forwarders**.

To learn more about each upgrade path and the order in which to perform each upgrade task, see the [Upgrade Path Checklists for Operations Manager](#).

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

You should also verify that the agents meet the supported configurations for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#).



Note

If you attempt to upgrade a 32-bit agent that was installed on a 64-bit machine, the upgrade of the agent will fail.



Note

If UAC is enabled, you must run the agent upgrade from an elevated command prompt.



Note

Information about upgraded agents might not appear in the Operations console for up to 60 minutes after performing the upgrade.

Upgrading Push-Installed Agents

▶ To upgrade push-installed Windows agents by using the Operations console

1. If you are upgrading agents in a distributed management group or if you have added a secondary management server, log on to the computer hosting the Operations Manager 2007 R2 Operations console. Use an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 R2 management group.
If you are upgrading agents in a single-server management group, log on to the computer hosting the Operations Manager Operations console by using an account that is a

member of the Operations Manager Administrators role.

2. In the Operations console, click **Administration**.



Note

When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the management server to which you want to connect.

3. In the **Administration** workspace, in the navigation pane under **Device Management**, click **Pending Management**.
4. In the **Pending Management** pane, under **Type: Agent Requires Update**, right-click each agent-managed computer listed, and then click **Approve**.



Warning

You should not approve more than 200 agents at one time.

5. In the **Update Agents** dialog box, enter the administrator account credentials, and then click **Update**. The upgrade status is displayed in the **Agent Management Task Status** dialog box.
6. When the upgrade is completed, click **Close**.

Upgrading Manually Installed Agents

▶ To upgrade a manually installed Windows agent by using the Setup Wizard

1. Log on to the computer that hosts the agent with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. Run **Setup.exe** from the System Center 2012 – Operations Manager installation media.
3. On the first page of the Setup Wizard, click **Local agent**. When the **Welcome to the System Center 2012 - Operations Manager Agent Upgrade Wizard** page opens, click **Next**.
4. In the **System Center 2012 - Operations Manager Agent Setup** dialog box, click **Upgrade**. The status page displays the progress of the upgrade.
5. When the **Completing the System Center 2012 - Operations Manager Agent Setup wizard** page appears, click **Finish**.

▶ To upgrade a manually installed Windows agent by using the Command Prompt window

1. Log on to the computer hosting the agent with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change directory to **agent**, and then change directory again to **AMD64**, **i386**, or **ia64**, as appropriate for the current system.
4. Run the following command, where D:\ is the location for the upgrade log file.



Note

If you upgrade manually installed agents that also run the AVIcode 5.7 agent (or

earlier versions of the AVICode agent), you must include the option: **NOAPM=1** in the command. For more information, see [Install Agent Using the Command Line](#).

```
msiexec /i MOMAgent.msi /qn /l*v D:\logs\AgentUpgrade.log
```

Verifying Windows Agent Upgrade

▶ To verify the Windows agent upgrade

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **Agent Managed**.
3. In the **Agent Managed** pane, verify that the value listed in the **Version** column is 7.0.85xx.x, where x is any positive integer.



Note

It can take up to one hour for the console to show the updated version of the agent.

Upgrading UNIX and Linux Agents

▶ To upgrade UNIX and Linux agents in a distributed management group

1. Log on to the root management server hosting the Operations Manager 2007 R2 Operations console with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 R2 management group.
2. In the Operations console, click **Administration**.
3. At the bottom of the navigation pane, select the **Discovery Wizard** link.
You must initiate the upgrade by running the Discovery Wizard in Operations Manager 2007 R2 on agents that have been moved to a secondary management server that has been upgraded to Operations Manager. There is no **Pending Management** feature for UNIX and Linux agents in either version.
4. In the **Computer and Device Management Wizard**, select **Discovery Type**, select **Unix/Linux Discovery Wizard**, and then click **Next**.
5. On the **Discovery Method** page, click **Add**.
6. On the **Define discovery criteria** page, type the credentials and necessary information to locate the secondary management server, and then click **OK**.
7. On the **Discovery Method** page, click **Add** to add the secondary management server to the **Discovery Scope** list.
8. In the **Management Server** list, select the secondary management server that will monitor the agents.
9. Click **Discover** to initiate system discovery.
10. On the **Discovery results** page, the wizard detects that the agents are already managed and that an upgrade is available. Continue with the upgrade.
11. Click **Done** to close the wizard.

Any existing Run As profiles and Run As accounts continue to have valid configurations. For information about changes to Run As profiles and accounts for UNIX and Linux monitoring in System Center 2012 – Operations Manager, see [Accessing UNIX and Linux Computers in System Center 2012 - Operations Manager](#).

You can specify the resource pool that manages a particular UNIX or Linux computer and allows you to create a resource pool dedicated to managing only UNIX and Linux computers. For more information see [Managing Resource Pools for UNIX and Linux Computers](#).

► To upgrade UNIX and Linux agents in a single-server management group by using the Operations console

1. On the management server that was upgraded to System Center 2012 – Operations Manager, configure at least an Agent Maintenance account (for a Run As account) for the predefined UNIX and Linux profiles. Optionally configure other accounts.

Note

If any UNIX or Linux agents are not upgraded to the System Center 2012 – Operations Manager version, and a Run As account is configured for a normal user account on the UNIX or Linux computer that uses sudo elevation, the elevation fails under that circumstance. A normal user account does not have root-level access or special permissions, but allows monitoring of system processes and of performance data. For more information about credentials and elevation, see [Accessing UNIX and Linux Computers in Operations Manager 2012](#).

2. Run the **UNIX/Linux Upgrade Wizard**. For more information, see [Upgrading and Uninstalling Agents on UNIX and Linux Computers](#).

► To manually upgrade UNIX and Linux agents in a single-server management group

1. Copy the System Center 2012 – Operations Manager agent package to the managed UNIX or Linux computer. The default location of the agent package is C:\Program Files\System Center 2012\Operations Manager\Server\AgentManagement\UnixAgents.
2. Run the appropriate package upgrade command. For example, the following command upgrades the agents on a Linux computer.

```
rpm -Uvh <filename>.rpm
```

► To verify the UNIX or Linux agent upgrade

1. In the Operations console, in the navigation pane, click the **Administration** button.
2. Under **Device Management**, click **UNIX/Linux Computers**.
3. In the **Agent Managed** pane, verify that the value listed in the **Version** column is 1.2.0-xxx, where x is any positive integer.

Note

It can take up to one hour for the console to show the updated version of the

agent.

See Also

[Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group](#)

[Upgrading Operations Manager 2007 R2 Agents in a Distributed Management Group](#)

[Upgrading a Distributed Operations Manager 2007 R2 Environment](#)

[Upgrade Path Checklists for Operations Manager](#)

How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS

You upgrade your System Center Operations Manager 2007 R2 management group to System Center 2012 – Operations Manager from the root management server (RMS) when the computer hosting the Operations Manager 2007 R2 RMS meets the minimum supported configurations for System Center 2012 – Operations Manager.

You should first upgrade other features, such as secondary management servers, agents, and gateways before running the final upgrade on the management group. For more information about each upgrade path and the order in which to perform each upgrade task, see [Upgrade Path Checklists for Operations Manager](#).

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

If the computer hosting the RMS does not meet the minimum supported configurations, you must run upgrade from a secondary management server. For more information, see [How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server](#).

► To upgrade a management group from an RMS

1. Log on to the computer that hosts the root management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer. You also require SQL Server Administrator rights on both the operational database server and the data warehouse server.
2. On the System Center 2012 – Operations Manager media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started, System Center 2012 - Operations Manager Upgrade** page, review the features that will be upgraded and added, and click **Next**.



Important

The Operations Manager data warehouse will be added if it does not already exist.

4. On the **Getting Started, Please read the license terms** page, review the license terms and select the option **I have read, understood, and agree with the license terms**, and

then click **Next**.

5. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
6. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.



Note

SQL Server Full Text Search must be enabled. For more information, see [Full-text Search Overview](#).

7. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
8. If a data warehouse was not already installed, it is created, and you must configure it as follows:
 - a. In the **Configuration, Configure the data warehouse database** page, type the name and instance of the SQL Server database server for the database server that will host the System Center 2012 – Operations Manager data warehouse database in the **Server name and instance name** box.
 - b. Accept the default value of **Create a new data warehouse database** or select an existing data warehouse.
 - c. In the **Database name**, **Database size (MB)** **Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.



Note

These paths do not change if you connect to a different instance of SQL Server.

9. On the **Configuration, Configure Operations Manager accounts** page, we recommend that you use the **Domain Account** option for the **System Center Configuration service and System Center Data Access service** accounts. Before the account is validated, an error icon appears to the left of the **Domain\Username** box.
10. Enter the credentials for a domain account in each box. The error icons disappear after account validation. Click **Next**.
11. On the **Configuration, Ready To Upgrade** page, click **Upgrade**.
12. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

▶ **To upgrade a management group from an RMS by using the Command Prompt window**

1. Log on to the computer that hosts the root management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer. You also need SQL Server Administrator rights on both the operational database server and the data warehouse server.
2. Open a Command Prompt window by using the **Run as administrator** option.

3. Change the path to where the System Center 2012 – Operations Manager Setup.exe file is located.

 **Important**

The following commands assume that you specified the Local System account for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.

```
/DASAccountUser: <domain\username> /DASAccountPassword: <password>
```

If you installed a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

```
setup.exe /silent /upgrade  
/AcceptEndUserLicenseAgreement  
/UseLocalSystemDASAccount  
/DataReaderUser:<domain\user>  
/DataReaderPassword:<domain\user>
```

If you did not install a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

```
Setup.exe /silent /upgrade  
/AcceptEndUserLicenseAgreement  
/UseLocalSystemDASAccount  
/DWSqlServerInstance:<server\instance>  
/DWDatabaseName:<DW name>  
/DataReaderUser:<domain\username>  
/DataReaderPassword:<password>  
/DataWriterUser:<domain\username>  
/DataWriterPassword:<password>
```

See Also

[Upgrading a Distributed Operations Manager 2007 R2 Environment](#)

[Upgrade Path Checklists for Operations Manager](#)

How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server

You upgrade your System Center Operations Manager 2007 R2 management group to System Center 2012 – Operations Manager from a secondary management server when the computer hosting the Operations Manager 2007 R2 root management server (RMS) does not meet the minimum supported configurations for System Center 2012 – Operations Manager. For more

information, see [Supported Configurations for System Center 2012 - Operations Manager](#). You must first move the agents over to the secondary management server and gateway servers. For more information, see [How to Move Agents to an Operations Manager 2007 R2 Secondary Management Server \(Operations Manager Upgrade\)](#).

 **Important**

If you have a clustered Operations Manager 2007 R2 RMS, you might receive an error during the prerequisite check that indicates that the root management server still has devices reporting to it, even if you have moved the agents to a secondary management server. To resolve this, open the Operations console, and select the **Administration** workspace. In **Device Management**, select **Agentless Managed**. Right-click the agentless nodes, and then click **Delete**.

 **Note**

Before you follow any of these procedures, make sure that you verify that the servers in your Operations Manager 2007 R2 management group meet the minimum supported configurations for System Center 2012 – Operations Manager. This will help you determine whether you need to add any new servers to your management group before you upgrade. For more information, see [Supported Configurations for System Center 2012 – Operations Manager](#).

You should first upgrade other features, such as secondary management servers, agents, and gateways before running the final upgrade on the management group. If you have more than one secondary management server in your management group, we recommend that you upgrade from the secondary management server that has the simplest configuration. For example, if you have a management server that does not have any gateways, agents, or network devices, run upgrade from that management server. For more information about each upgrade path and the order in which to perform each upgrade task, see [Upgrade Path Checklists for Operations Manager](#).

If the computer hosting the RMS meets the minimum supported configurations, you can run upgrade on that server. For more information, see [How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS](#).

When you run upgrade from the secondary management server, the management server is marked as the RMS emulator, and the unsupported RMS is removed from the management group. The RMS emulator enables legacy management packs that rely on the RMS to continue to function in System Center 2012 – Operations Manager.

 **Important**

You must restore the encryption key on the secondary management server before you attempt to upgrade the management group. For more information, see [Restore the Encryption Key on the Secondary Management Server](#)

 **To upgrade a management group from a secondary management server**

1. Log on to the computer that hosts the secondary management server with an account

that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer. You also need SQL Server Administrator rights on both the operational database server and the data warehouse server.

2. Open a Command Prompt window as an administrator by using the **Run as administrator** feature.
3. Change to the path of the System Center 2012 – Operations Manager Setup.exe file, and run the following command.

```
setup.exe /upgrademanagementgroup
```

4. When the **System Center 2012 - Operations Manager** wizard opens, click **Install**.
5. On the **Getting Started, System Center 2012 - Operations Manager Upgrade** page, review the features that will be upgraded and added, and click **Next**.

 **Important**

The Operations Manager data warehouse is added if it does not already exist. The Operations Manager 2007 R2 root management server is removed from the management group.

6. On the **Getting Started, Please read the license terms** page, review the license terms and select the option **I have read, understood, and agree with the license terms**, and then click **Next**.
7. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.

 **Important**

If there are any issues with the upgrade, such as having agents still reporting to the RMS, the **Prerequisites** page appears with information about the issue and how to resolve it.

8. If the Prerequisites checker does not return any warnings or errors the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
9. If a data warehouse was not already installed, it is created, and you must configure it as follows:
 - a. In the **Configuration, Configure the data warehouse database** page, type the name and instance of the SQL Server database server that will host the Operations Manager data warehouse database in the **Server name and instance name** box.
 - b. Accept the default value of **Create a new data warehouse database**.
 - c. In the **Database name, Database size (MB) Data file folder**, and **Log file folder** boxes, we recommend that you accept the default values. Click **Next**.




Note

These paths do not change if you connect to a different instance of SQL Server.

10. On the **Configuration, Configure Operations Manager accounts** page, we

recommend that you use the **Domain Account** option for the **System Center Configuration service and System Center Data Access service** accounts, the **Data Reader account** and **Data Writer account**. Before the account is validated, an error icon appears to the left of the **Domain\Username** box.

11. Enter the credentials for a domain account in each box. The error icons disappear after account validation. Click **Next**.
12. If Windows Update is not enabled on the computer, the **Configuration, Microsoft Update** page appears. Select your options, and then click **Next**.
13. Review the options on the **Configuration, Ready to Upgrade** page, and then click **Upgrade**.
14. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

 **To upgrade a management group from a secondary management server by using the Command Prompt window**

1. Log on to the computer that hosts the secondary management server with an account that is a member of the Operations Manager Administrators role for your Operations Manager 2007 R2 management group and a local administrator on the computer.
2. Open a Command Prompt window as an administrator by using the **Run as administrator** option.
3. Change the path to where the System Center 2012 – Operations Manager Setup.exe file is located.

 **Important**

The following commands assume that you specified the Local System account for the Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead:

```
/DASAccountUser: <domain\username> /DASAccountPassword: <password>
```

If you installed a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

```
setup.exe /silent /upgrademanagementgroup  
/AcceptEndUserLicenseAgreement  
/UseLocalSystemDASAccount
```

If you did not install a data warehouse in your Operations Manager 2007 R2 management group, use the following command.

```
setup.exe /silent /upgrademanagementgroup  
/AcceptEndUserLicenseAgreement  
/UseLocalSystemDASAccount  
/DWSqlServerInstance:<server\instance>  
/DataReaderUser:<domain\username>
```

```
/DataReaderPassword:<password>  
/DataWriterUser:<domain\username>  
/DataWriterPassword:<password>
```

See Also

[Upgrading a Distributed Operations Manager 2007 R2 Environment](#)
[Upgrade Path Checklists for Operations Manager](#)

Upgrading or Installing Optional Features

When you upgrade to System Center 2012 – Operations Manager, there are optional features, such as a stand-alone operations console, web console, Reporting server, and ACS collector that you might want to upgrade. If they were not already installed in the System Center Operations Manager 2007 R2 management group, you might want to install the System Center 2012 – Operations Manager versions after you have completed upgrade.

Important

If you have a Reporting server installed on a root management server (RMS) that does not meet the supported configuration for System Center 2012 – Operations Manager, you will not be able to upgrade it. Instead, you can install a System Center 2012 – Operations Manager Reporting server after you have upgraded your management group.

The following list provides links to optional features you can upgrade.

- [How to Upgrade a Stand-Alone Operations Console from Operations Manager 2007 R2](#)
- [How to Upgrade a Web Console from Operations Manager 2007 R2](#)
- [How to Upgrade Reporting from Operations Manager 2007 R2](#)
- [How to Upgrade an ACS Collector from Operations Manager 2007 R2](#)

The following list provides links to optional features you can install.

- [How to Install the Operations Console](#)
- [How to Install the Operations Manager Web Console](#)
- [How to Install the Operations Manager Reporting Server](#)
- [How to Deploy ACS on a Secondary Management Server](#)

How to Upgrade a Stand-Alone Operations Console from Operations Manager 2007 R2

This procedure upgrades a stand-alone Operations console from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager. Perform this procedure locally on the computer that has a stand-alone Operations console installed. You should only upgrade stand-alone Operations consoles after you have upgraded your management group. You do not have to perform this procedure to upgrade Operations consoles that are installed locally on a management server. For more information about each upgrade path and the order in which to perform each upgrade task, see [Upgrade Path Checklists for Operations Manager](#).

Before you proceed, ensure that your server meets the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#).

▶ **To upgrade a stand-alone Operations console**

1. Log on to the computer that hosts the Operations console with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. On the Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started, System Center 2012 - Operations Manager Upgrade** page, click **Next**.
4. On the **Getting Started, Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that are returned by the Prerequisites checker, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
7. On the **Configuration, Ready To Upgrade** page, click **Upgrade**.
8. When the upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

▶ **To upgrade a stand-alone Operations console by using the Command Prompt window**

1. Log on to the computer that hosts the Operations console with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change to the path to the System Center 2012 – Operations Manager source media, and run the following command.

```
Setup.exe /silent /upgrade
```

▶ **To verify the Operations console upgrade**

1. On the Windows desktop, click **Start**, and then click **Run**.
2. Type **regedit**, and then click **OK**. The Registry Editor starts.

 **Caution**

Incorrectly editing the registry can severely damage your system. Before you make changes to the registry, you should back up any valued data that is on the computer.

3. Browse to the **HKey_Local_Machine\Software\Microsoft\Microsoft Operations Manager\3.0\Setup** key. If the value of the **UIVersion** entry is **7.0.85##.#**, where **#** is any positive integer, the Operations console was upgraded successfully.

See Also

[Upgrading a Distributed Operations Manager 2007 R2 Environment](#)

[Upgrade Path Checklists for Operations Manager](#)

How to Upgrade a Web Console from Operations Manager 2007 R2

If you have a stand-alone System Center Operations Manager 2007 R2 web console server, you can upgrade it to System Center 2012 – Operations Manager. If your web console server was on the same computer as a secondary management server that was upgraded, you must re-install the web console. For more information, see [How to Install the Operations Manager Web Console](#).



Note

When you upgrade the web console, any customizations that were made to the web.config file after the web console was installed will be reset.

For more information about each upgrade path and the order in which to perform each upgrade task, see [Upgrade Path Checklists for Operations Manager](#).

Before you proceed, ensure that your server meets the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#).

► To upgrade the web console server

1. Log on to the computer that hosts the web console server with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. On the System Center 2012 – Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started, System Center 2012 - Operations Manager Upgrade** page, review the features that will be upgraded, and then click **Next**.
4. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
7. If the root management server has not been upgraded or is unavailable, the **Configuration, Specify a management server** page appears. Enter the name of a System Center 2012 – Operations Manager management server that is to be used by the web console, and then click **Next**.
8. On the **Configuration, Specify a web site for use with the Web console** page, select the **Default Web Site**, or the name of an existing website. Select **Enable SSL** only if the website has been configured to use Secure Sockets Layer (SSL), and then click **Next**.
9. On the **Configuration, Select an authentication mode for use with the Web console** page, select your options, and then click **Next**.

10. When the **Ready to Upgrade** page appears, review the upgrade summary, and then click **Upgrade**.

▶ **To upgrade the web console server by using the Command Prompt window**

1. Log on to the computer that hosts the web console server with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the System Center 2012 – Operations Manager Setup.exe file is located, and run the following command.



Important

Use the `/WebConsoleUseSSL` parameter only if your website has Secure Sockets Layer (SSL) activated. For a default web installation, specify **Default Web Site** for the `/WebSiteName` parameter.



Note

If the web console reports to an unsupported or inaccessible root management server, you must also pass the following parameter:
`/ManagementServer:<servername>`.

```
setup.exe /silent /upgrade  
  
/WebsiteName: "<WebSiteName>" [/WebConsoleUseSSL]  
  
/WebConsoleAuthorizationMode: [Mixed|Network]
```

See Also

[Upgrading a Distributed Operations Manager 2007 R2 Environment](#)

[Upgrade Path Checklists for Operations Manager](#)

How to Upgrade Reporting from Operations Manager 2007 R2

Use this procedure to upgrade a stand-alone Reporting server from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager. You run upgrade on the Reporting server after you have upgraded the management group. For more information about each upgrade path and the order in which to perform each upgrade task, see [Upgrade Path Checklists for Operations Manager](#).

Before you proceed, ensure that your server meets the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#).

If you upgraded your management group from the secondary management server, the System Center Operations Manager 2007 R2 root management server (RMS) was removed during the upgrade process. As a result, you will have to manually edit the configuration file for the Reporting server (`rsreportserver.config`). If you attempt to upgrade Operations Manager Reporting

without making this change, the Upgrade Wizard will report a critical prerequisite issue, because Operations Manager is unable to connect to the reporting server.

 **Important**

If you upgraded your management group from the RMS, then you do not have to manually update the configuration file for the Reporting server.

 **To Modify the Reporting Server Configuration File**

1. On computer that hosts the Reporting server you plan to upgrade, open the **rsreportserver.config** file using Notepad. The path is typically **C:\Program Files\Microsoft SQL Server\MSRS10.MSSQLServer\Reporting Services\ReportServer**, where MSSQLServer is the name of the SQL Server instance.
2. From the **Edit** menu, click **Find**. Search for **<ServerName>**.

 **Note**

The **<ServerName>** element appears in two places in the configuration file, in the Security Extension and in the Authentication Extension.

3. Replace the name of the management server from the old RMS name, with the name of an upgraded management server.
4. Search for **<ServerName>** again, and update the server name.
5. Save and close the configuration file.
6. If the Setup wizard is open, you should close it and restart the upgrade process.

 **To upgrade the Reporting server**

1. Log on to the computer that hosts the Reporting server with an account that is a member of the Operations Manager 2007 R2 Administrators role for your Operations Manager 2007 R2 management group.
2. On the System Center 2012 – Operations Manager source media, run **Setup.exe**, and then click **Install**.
3. On the **Getting Started, System Center 2012 - Operations Manager Upgrade** page, review the features that will be upgraded. In this case, it is Operations Manager 2007 R2 Reporting. Click **Next**.
4. On the **Select installation location** page, accept the default value of **C:\Program Files\System Center 2012\Operations Manager**, or type in a new location or browse to one. Then click **Next**.
5. On the **Prerequisites** page, review and address any warnings or errors that the Prerequisites checker returns, and then click **Verify Prerequisites Again** to recheck the system.
6. If the Prerequisites checker does not return any warnings or errors, the **Prerequisites, Proceed with Setup** page appears. Click **Next**.
7. If the root management server has not been upgraded or is unavailable, the **Configuration, Specify a management server** page appears. Enter the name of a System Center 2012 – Operations Manager management server that is to be used by the

- Reporting server, and then click **Next**.
8. On the **Ready to Upgrade** page, review the options, and then click **Upgrade**.
 9. When upgrade is finished, the **Upgrade complete** page appears. Click **Close**.

▶ **To upgrade the Reporting server by using the command prompt**

1. Log on to the computer that hosts the Reporting server with an account that is a member of the Operations Manager 2007 R2 Administrators role for your Operations Manager 2007 R2 management group.
2. Open a Command Prompt window by using the **Run as Administrator** option.
3. Change the path to where the System Center 2012 – Operations Manager Setup.exe file is located, and run the following command:



Note

If the Reporting server reports to an unsupported or inaccessible root management server, you must also pass the following parameter:

```
/ManagementServer: <ManagementServerName>.  
  
setup.exe /silent /upgrade
```

See Also

[Upgrading a Distributed Operations Manager 2007 R2 Environment](#)

[Upgrade Path Checklists for Operations Manager](#)

How to Upgrade an ACS Collector from Operations Manager 2007 R2

Perform this procedure to upgrade the Audit Collection Services (ACS) Collector from System Center Operations Manager 2007 R2 to System Center 2012 – Operations Manager locally on the ACS Collector. During this procedure, the ACS database is also upgraded without any additional steps.



Note

A computer that hosts an ACS Collector must also be an Operations Manager management server or gateway server. You must upgrade the management servers before you upgrade the ACS Collector. For more information about each upgrade path and the order in which to perform each upgrade task, see [Upgrade Path Checklists for Operations Manager](#).

Before you proceed, ensure that your server meets the minimum supported configurations for System Center 2012 – Operations Manager. For more information, see [Supported Configurations for System Center 2012 - Operations Manager](#).

▶ **To upgrade an ACS Collector**

1. Log on to the computer that hosts the ACS Collector with an Operations Manager Administrators role account for your Operations Manager 2007 R2 management group.

2. On the System Center 2012 – Operations Manager media, run **Setup.exe**.
3. In the **Install** section, click **Audit collection services**. The Audit Collection Services Collector Setup wizard starts.
4. On the **Welcome to the Audit Collection Services Collector Setup Wizard** page, click **Next**.
5. In the **ACS Collector Maintenance** page, select Update the ACS collector configuration, and then click **Next**.
6. On the **Database Installation Options** page, select **Use an existing database**, and then click **Next**.
7. On the **Data Source** page, type the name that you used as the Open Database Connectivity data source name for your ACS database in the **Data source name** box. By default, this name is **OpsMgrAC**. Click **Next**.
8. On the **Database** page, if the database is on a separate server than the ACS Collector, click **Remote Database Server**, and then type the computer name of the database server that will host the database for this installation of ACS. Otherwise, click **Database server running locally**, and then click **Next**.
9. On the **Database Authentication** page, select one authentication method. If the ACS Collector and the ACS database are members of the same domain, you can select **Windows authentication**; otherwise, select **SQL authentication**, and then click **Next**.

**Note**

If you select **SQL Server Authentication** and click **Next**, the **Database Credentials** page appears. Enter the name of the user account that has access to the SQL Server in the **SQL login name** box and the password for that account in the **SQL password** password box, and then click **Next**.

10. The **Summary** page displays a list of actions that the installation program will perform to upgrade ACS. Review the list, and then click **Next** to begin the installation.

**Note**

If a **SQL Server Login** dialog box appears and the database authentication is set to **Windows Authentication**, select the correct database, and then verify that the **Use Trusted Connection** check box is selected. Otherwise, clear it, enter the SQL Server login name and password, and then click **OK**.

11. When the upgrade is finished, click **Finish**.

See Also

[Upgrading a Distributed Operations Manager 2007 R2 Environment](#)

[Upgrade Path Checklists for Operations Manager](#)

Post-Upgrade Tasks when Upgrading from Operations Manager 2007 R2

After you have completed the upgrade process for System Center 2012 – Operations Manager, you must perform a number of post-upgrade tasks.

Post-Upgrade Tasks

The following table shows the tasks that you need to complete after you have upgraded to System Center 2012 – Operations Manager. It also indicates when to perform the task.

Task	When to the Perform Task
Re-enable the Notification Subscriptions.	After you complete the upgrade tasks in any upgrade path.
Restart or Re-enable the Connector Services	After you complete the upgrade tasks in any upgrade path, and only if the connector services are installed.
Uninstall the Old RMS	Only if you upgrade the management group on the secondary management server.
Update Overrides	After you upgrade the management group
Verify That the Upgrade Was Successful	After you complete the upgrade tasks in any upgrade path.
Run SQL Query on each Management Group	Run SQL query on each management group to clean up the Localizedtext table and the Publishmessage table.
Assign UNIX/Linux Agents to a Resource Pool	After you complete the upgrade tasks in any upgrade path.

Re-enable the Notification Subscriptions.

After the upgrade has finished, use the following procedure to re-enable subscriptions.

To re-enable the subscriptions

1. Open the Operations console by using an account that is a member of the Operations Manager Administrators role for the System Center 2012 – Operations Manager management group.
2. In the Operations console, in the navigation pane, click the **Administration** button.



Note

When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** text box, type the name of the System Center 2012 – Operations Manager management server to which you want to connect.

3. In the **Administration** pane, under **Notifications**, click **Subscriptions**.
4. In the **Actions** pane, click **Enable** for each subscription listed.

Restart or Re-enable the Connector Services

Refer to the third-party documentation for any installed connectors to determine if the connectors are supported for System Center 2012 – Operations Manager.

To restart a connector service

1. On the taskbar, click **Start**, click **Administrative Tools**, and then click **Services**.
2. In the **Name** column, right-click the connector that you want to restart, and then click **Start**.

Uninstall the Old RMS

If you have upgraded to System Center 2012 – Operations Manager from the secondary management server because the RMS did not meet the supported configurations for System Center 2012 – Operations Manager, the RMS is removed from the management group during upgrade. You can then uninstall the old root management server (RMS).



Note

If you upgraded from the secondary management server, you can build a new management server with the same Windows computer name as the old RMS, rather than change the configuration settings to point to the new management server.

To uninstall the old RMS

1. Log on to the computer hosting the RMS with an account that has local administrator permissions.
2. On the taskbar, click **Start**, and then click **Control Panel**, and then run **Programs and Features**.
3. Right-click Operations Manager 2007 R2, and then click **Uninstall**.
4. In the **Program and Features** dialog box, click **Yes** to confirm that you want to uninstall.

Update Overrides

If you created any overrides for the Active Directory Integration rules, you must recreate them after the management group upgrade is complete. Delete the old override, and then create a new, matching override that targets the Active Directory Assignment Resource Pools.

Verify That the Upgrade Was Successful

Perform the following tasks to verify that the upgrade was successful.

- Check the health state of the management servers and agents in the Health Service Watcher state view. In the **Administration** workspace of the Operations console, ensure that the management servers and agents are healthy. In the **Monitoring** workspace, check if there are any alerts related to the management group health.
- Review the event logs of all the management servers for new errors.
- Sort alerts by the last-modified column to review the new alerts.
- Check the CPU utilization and disk I/O on your database servers to ensure that they are functioning normally.

- If the Reporting feature is installed, click Reporting, and then run a generic performance report to ensure that Reporting is functioning correctly.
- Re-deploy any agents that you uninstalled during the upgrade process.

Run SQL Query on each Management Group

Run the following SQL query on the Operational database in each management group to clean up the Localizedtext table and the Publishmessage table.

```
-- Create a temporary table to quickly find a PublisherId when you know the MessageId.
BEGIN TRY
CREATE TABLE #PublisherMessageReverseIndex(MessageStringId UNIQUEIDENTIFIER,
      MessageId INT)
CREATE CLUSTERED INDEX #PublisherMessageReverseIndex_CI ON
#PublisherMessageReverseIndex(MessageStringId)
INSERT INTO #PublisherMessageReverseIndex (MessageStringId, MessageId)
SELECT MessageStringId, MessageId
FROM dbo.PublisherMessages

-- Create a temporary table of message lengths, message IDs, and message hashes with the
-- MessageStringId to quickly determine whether a message is duplicated. Index the table.

CREATE TABLE #LTHashStrings (MessageStringId UNIQUEIDENTIFIER,
      LTValueLen INT,
      LTValueHash VARBINARY(32),
      MessageId INT NULL)
CREATE CLUSTERED INDEX #LTHashStrings_CI ON #LTHashStrings(MessageStringId)
CREATE NONCLUSTERED INDEX #LTHashStrings_NCI1 ON #LTHashStrings(LTValueLen, MessageId,
LTValueHash)

-- Create a temporary table for the orphaned PublisherStrings that you find. Orphaned
PublisherStrings
-- are rows in PublisherMessages whose corresponding events have already been groomed.
They still
-- have corresponding rows in LocalizedText. Do not add rows for PublisherMessages; they
are not
-- for duplicated messages.
```

```

CREATE TABLE #OrphanedPublisherStrings (PublisherId UNIQUEIDENTIFIER,
MessageStringId UNIQUEIDENTIFIER)
CREATE CLUSTERED INDEX #OrphanedPublisherStrings_CI ON
#OrphanedPublisherStrings (MessageStringId)

-- Create a temporary table so that you can determine whether a PublisherMessages row
still
-- has a corresponding event. These events do not have an index on the PublisherId, so do
-- not query the EventAllView. If a PublisherId occurs multiple times in the event
tables,
-- it is only needed one time in the temp table; therefore, the unique clustered index
-- must contain IGNORE_DUP_KEY. This keeps the temporary table relatively small and saves
-- time when you want to see the orphaned PublisherMessages.

CREATE TABLE #EventAllPublishers (PublisherId UNIQUEIDENTIFIER)
CREATE UNIQUE CLUSTERED INDEX #EventAllPublishers_CI ON #EventAllPublishers (PublisherId)
WITH (IGNORE_DUP_KEY = ON)

-- Populate the temporary table by scanning EventAllView one time.
INSERT INTO #EventAllPublishers(PublisherId)
SELECT PublisherId
FROM EventAllView

-- Populate the first temporary table to determine which messages are duplicated.
INSERT INTO #LTHashStrings (MessageStringId, LTValueLen, LTValueHash, MessageId)
SELECT LTStringId, len(LTValue), HashBytes('SHA1', LTValue), MessageId
FROM dbo.LocalizedText LT
JOIN #PublisherMessageReverseIndex PM ON PM.MessageStringId = LTStringId

-- Create the second table to determine which messages are duplicated.
CREATE TABLE #LTCountByMessage( LTValueLen INT,
MessageId INT,
LTValueHash VARBINARY(32),

```

```

MsgCount INT)

CREATE CLUSTERED INDEX #LTCountByMessage_CI ON #LTCountByMessage(LTValueLen, MessageId,
LTValueHash)

-- Populate second message for duplicate message detection by scanning the INDEX of
-- the first one and by doing a grouped count.
INSERT INTO #LTCountByMessage (LTValueLen, MessageId, LTValueHash, MsgCount)
SELECT LTValueLen, MessageId, LTValueHash, COUNT(1)
FROM #LTHashStrings
GROUP BY LTValueLen, MessageId, LTValueHash

-- You are now set up to detect both orphaned PublisherStrings and duplicated messages
-- by joining to our relatively small (and correctly indexed) temporary tables.
-- Determine the OrphanedPublisherStrings that have duplicate messages.
INSERT INTO #OrphanedPublisherStrings (PublisherId, MessageStringId)
SELECT PM.PublisherId, PM.MessageStringId
FROM dbo.PublisherMessages PM
JOIN #LTHashStrings LTS ON (LTS.MessageStringId = PM.MessageStringId AND LTS.MessageId =
PM.MessageId)
JOIN #LTCountByMessage LTC ON (LTC.LTValueLen = LTS.LTValueLen AND
LTC.MessageId = LTS.MessageId AND LTC.LTValueHash = LTS.LTValueHash)
WHERE PM.PublisherId NOT IN (SELECT PublisherId FROM #EventAllPublishers) AND
LTC.MsgCount > 1

-- Deleting all the OrphanedPublisherStrings and all the corresponding LocalizedText rows
-- at one time may be too large for the transaction log to handle. Create a numbered
-- or ordered table so that you can delete them in relatively small batches and not
-- overtax the transaction log.
CREATE TABLE #NumberOrphanPublisherStrings(OrphanNum INT IDENTITY,
PublisherId UNIQUEIDENTIFIER,
MessageStringId UNIQUEIDENTIFIER)
CREATE CLUSTERED INDEX #NumberOrphanPublisherStrings_CI on
#NumberOrphanPublisherStrings(OrphanNum)

```



```

-- Populate the numbered table.
INSERT INTO #NumberOrphanPublisherStrings (PublisherId, MessageStringId)
SELECT PublisherId, MessageStringId FROM #OrphanedPublisherStrings
END TRY
BEGIN CATCH
GOTO Error
END CATCH

-- Set up variables so that you can delete the orphaned rows.
-- If the transaction log fills up, try to reduce the @OrphanIncrement value,
-- which controls the number of rows that are delete at the same time.
DECLARE @OrphanNum INT
DECLARE @OrphanIncrement INT
DECLARE @OrphanLimit INT
SET @OrphanNum = 0
SET @OrphanIncrement = 10000
SELECT @OrphanLimit = MAX(OrphanNum) FROM #NumberOrphanPublisherStrings
BEGIN TRY
WHILE @OrphanNum < @OrphanLimit
BEGIN
DELETE dbo.LocalizedText FROM
#NumberOrphanPublisherStrings OPS JOIN dbo.LocalizedText LT
ON LT.LTStringId = OPS.MessageStringId
WHERE OPS.OrphanNum >= @OrphanNum AND OPS.OrphanNum < @OrphanNum + @OrphanIncrement
DELETE dbo.PublisherMessages FROM
#NumberOrphanPublisherStrings OPS JOIN dbo.PublisherMessages PM
ON PM.PublisherId = OPS.PublisherId
WHERE OPS.OrphanNum >= @OrphanNum AND OPS.OrphanNum < @OrphanNum + @OrphanIncrement
SET @OrphanNum = @OrphanNum + @OrphanIncrement
END
END TRY
BEGIN CATCH
GOTO Error
END CATCH

```

```

Error:
IF @@ERROR <> 0

    SELECT

        ERROR_NUMBER() AS ErrorNumber,

        ERROR_MESSAGE() AS ErrorMessage;

-- Try to drop all the temporary tables
BEGIN TRY

IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#PublisherMessage%')

DROP TABLE #PublisherMessageReverseIndex

IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#OrphanedPublisherStrings%')

DROP TABLE #OrphanedPublisherStrings

IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#LTHashStrings%')

DROP TABLE #LTHashStrings

IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#EventAllPublishers%')

DROP TABLE #EventAllPublishers

IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#LTCountByMessage%')

DROP TABLE #LTCountByMessage

IF EXISTS (SELECT 1 FROM tempdb.INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE
'#NumberOrphanPublisherStrings%')

DROP TABLE #NumberOrphanPublisherStrings

END TRY

BEGIN CATCH

    SELECT

        ERROR_NUMBER() AS ErrorNumber,

        ERROR_MESSAGE() AS ErrorMessage;

END CATCH

```

Assign UNIX/Linux Agents to a Resource Pool

After completing the upgrade, UNIX/Linux agents must be assigned to a resource pool to enable highly-available monitoring and agent administration. For more information on creating resource pools, see **How to Create a Resource Pool**.



1. Open the Operations console by using an account that is a member of the Operations Manager Administrators role for the **om12short** management group.
2. In the Operations console, in the navigation pane, click the **Administration** button.
3. In the **Administration** pane, under **Device Management**, click **UNIX/Linux Computers**.
4. Select the UNIX/Linux computers to assign to a resource pool, and in the **Actions** pane, click **Change Resource Pool**.
5. Complete the **Change Resource Pool** wizard to assign the computers to the selected resource pool.

Upgrading to System Center 2012 - Operations Manager by Using the Command Prompt Window

You can upgrade to System Center 2012 – Operations Manager by using the **setup.exe** command in the Command Prompt window. Gateway and agent upgrades require the use of MOMGateway.msi and MOMAgent.msi. For information about supported configuration requirements of System Center 2012 – Operations Manager, see [Supported Configurations for System Center 2012 – Operations Manager](#).

Command-line Parameters for setup.exe

The following table lists the command-line parameters for installing features of System Center 2012 – Operations Manager.



Note

If the parameter contains a colon, a value is required. Otherwise, it is simply a switch.

Parameter	Value
/silent	Does not display the installation wizard during upgrade.
/upgrade	Used to upgrade all features of Operations Manager, if they meet the minimum supported configuration requirements.
/upgrademanagementgroup	Used to upgrade the management group from the secondary management server if the Root

Parameter	Value
	<p>Management Server does not meet the supported configuration requirements.</p> <p>Used after you have upgraded other features, such as secondary management servers, agents, and gateways.</p>
/UseLocalSystemDASAccount	Used to specify the Local System for the Data Access service account.
/DASAccountUser:	<p>The domain and user name of the Data Access service account.</p> <p>Used if you did not specify the Local System.</p>
/DASAccountPassword:	<p>The password for the Data Access service account.</p> <p>Used if you did not specify the Local System.</p>
/AcceptEndUserLicenseAgreement	Used to specify that you accept the End User License Agreement (EULA). This is only required when you are upgrading the System Center Operations Manager 2007 R2 management group from the Root Management Server (RMS) or the secondary management server.
/ManagementServer:	Used to specify the name of the management server to associate with a web console and/or Reporting server that you are upgrading. Only required if the web console and/or Reporting server is associated with an RMS that cannot be upgraded.
/DWSqlServerInstance:	The data warehouse server and instance (<server\instance>).
/DWDatabaseName:	The name of the data warehouse database.
/DataReaderUser:	The domain and user name of the data reader account.
/DataReaderPassword:	The password for the data reader account.
/DataWriterUser:	The domain and user name of the data writer account.
/DataWriterPassword:	The password for the data writer account.

Parameter	Value
/WebSiteName:	The name of the website. If default web installation, specify " Default Web Site ". Used for web console upgrades.
/WebConsoleUseSSL	Specify only if your website has Secure Sockets Layer (SSL) activated. Used for web console upgrades.
/WebConsoleAuthorizationMode:	Mixed: Used for intranet scenarios. Network: Used for extranet scenarios. Used for web console upgrades.

For examples of command lines for upgrading the various features of Operations Manager 2007 R2 to System Center 2012 – Operations Manager, see the following:

- [How to Upgrade an Operations Manager 2007 R2 Single-Server Management Group](#)
- [Upgrading Agents in an Operations Manager 2007 R2 Single-Server Management Group](#)
- [How to Upgrade a Secondary Management Server from Operations Manager 2007 R2](#)
- [How to Upgrade a Gateway Server from Operations Manager 2007 R2](#)
- [How to Upgrade Agents from Operations Manager 2007 R2](#)
- [How to Upgrade a Management Group from an Operations Manager 2007 R2 RMS](#)
- [How to Upgrade a Management Group from an Operations Manager 2007 R2 Secondary Management Server](#)
- [How to Upgrade a Stand-Alone Operations Console from Operations Manager 2007 R2](#)
- [How to Upgrade a Web Console from Operations Manager 2007 R2](#)
- [How to Upgrade Reporting from Operations Manager 2007 R2](#)

Maintaining the System Center 2012 - Operations Manager Infrastructure

After you have deployed or upgraded to System Center 2012 – Operations Manager, you might want to make changes to your Operations Manager infrastructure, such as backing up or moving a database. This section of the [Deploying System Center 2012 - Operations Manager](#) provides information about maintaining your installation of Operations Manager.

- [Backup and Disaster Recovery in Operations Manager](#)
- [Making Changes to an Operations Manager Environment](#)
- [Sending Data to Microsoft](#)

Backup and Disaster Recovery in Operations Manager

As part of your maintenance plan, it is important to include a backup plan. This plan should be thoroughly tested and documented in a simulated environment by using production backups. Ensure that the System Center 2012 – Operations Manager backup plan is integrated in any existing backup procedures in the organization.



Note

Before reading this section, be sure to review [Planning the System Center 2012 - Operations Manager Deployment](#) to understand the components of Operations Manager and to learn how to prepare for failure recovery.

Decide on the following issues:

- What to back up
- How often to back up
- Whether to perform complete or incremental backups
- How and when to practice restore procedures

After you decide what the best backup strategies for your System Center 2012 – Operations Manager environment, develop and document a backup plan to become part of the overall disaster recovery plan.

We strongly recommend that you test your backup and restore procedures thoroughly. Testing helps ensure that you have the required backups to recover from various failures and that staff can run the procedures smoothly and quickly if a failure occurs.

You can use a test environment including all the Operations Manager features to test your backup and restore processes.



Note

The overall backup practices in your organization might include backing up the disk drives that the Operations Manager is installed on. When backing up those disk drives, including the management servers, ensure to exclude the <Installed Partition>\Program Files\System Center 2012\Operations Manager\Server\Health Service State folder.

In This Section

[Complete and Incremental Backups in Operations Manager](#)

[Backup File Naming Conventions in System Center 2012 - Operations Manager](#)

[Back Up System Center 2012 - Operations Manager](#)

Complete and Incremental Backups in Operations Manager

You must ensure that database backups are as recent and complete as possible. This topic provides information to help you decide how to incorporate both complete and incremental database backups into an overall backup plan.



Note

By default, the report server database uses a full recovery model. Other Operations Manager databases use a simple recovery model. For more information about backup options, see [Backup Overview \(SQL Server\)](#).

Complete Database Backups

A complete database backup captures the entire database, including all entries in the transaction log, and excluding any unallocated extents in the files. Pages are read directly from disk to increase the speed of the operation.

You can re-create a database from its backup in one step by restoring a backup of the database. The restore process overwrites the existing database or creates the database if it does not exist. The restored database matches the state of the database at the time the backup finished, without any uncommitted transactions. Uncommitted transactions are rolled back when the database is restored.

A complete database backup uses more storage space per backup than transaction log and incremental database backups. Consequently, complete database backups take longer and therefore are typically created less frequently than incremental database or transaction log backups.

Incremental Database Backups

An incremental (differential) database backup records only the data that has changed after the last database backup. You can frequently make incremental backups of a database because incremental database backups are smaller and faster than complete database backups. Making frequent incremental backups decreases your risk of losing data.

In case of database failure, you can use incremental database backups to restore the database to the point at which the incremental database backup was finished.

Transaction Log Backups

The transaction log is a serial record of all the transactions that have been performed against the database after the transaction log was last backed up. With transaction log backups, you can restore the database to a specific point in time (for example, before entering unwanted data) or to the point of failure.

When restoring a transaction log backup, Microsoft SQL Server rolls forward all changes recorded in the transaction log. When SQL Server reaches the end of the transaction log, the state of the database is exactly as it was at the time the backup operation started. If the database is recovered, SQL Server then rolls back all transactions that were incomplete when the backup operation started.



Note

The data warehouse database uses a simple recovery model that truncates all transactions after completion. This means that backing up the log file is insufficient. Perform a complete database file backup.

For more information about recovery models, see [Recovery Model Overview](#).

Backup File Naming Conventions in System Center 2012 - Operations Manager

Correct use of naming conventions for backup files helps you distinguish between them. Backup files are unique based on the management group that they back up and the time that the backup was created. Consistent use of a standard naming convention can help you avoid the unintentional restoration of a backup to the wrong management group or restoring a backup from the wrong time.

Database File Naming Conventions

There might be multiple management groups in your Operations Manager environment; therefore, ensure to include the management group name or some distinguishing name in the database backup file names.

You can also include other information in the file name, such as the database name, date, and type of backup. For example, a file name might be formatted as follows:

OpsMgrDB_DIFFERENTIAL_<management group name>_7_15_2011 or
REPORTING_FULL_<management group name>_7_15_2011.

Custom Management Pack Naming Conventions

If your monitoring infrastructure consists of multiple management groups, it is very likely that the configuration of management packs and their overrides vary across those management groups. Therefore, implementing a standard naming convention for custom management packs helps prevent the same problems as using a standard naming convention for databases.

Include the management group name or some distinguishing name in the .xml file name for these backups. Also include the version of the sealed management pack for which the custom management pack contains overrides and other information in the file name, such as the date.

For example, a file name might be in the following format: **<management group name>_<Management pack name>_<Management pack version>_7_15_2011.xml.**

Back Up System Center 2012 - Operations Manager

To preserve data in case of a failure, you must have a recent backup of System Center 2012 – Operations Manager databases and other important data as listed in this topic.

Data to Back Up

To ensure your ability to correctly preserve and restore your Operations Manager environment, you should back up the following key items:

- Operational database, data warehouse database, and the Audit Collection Services (ACS) database
- Custom management packs
- Custom report definition files and computer certificates
- [Recommended Backup Schedule for System Center 2012 - Operations Manager](#)
- [How to Back Up Custom Management Packs](#)
- [How to Schedule Backups of System Center 2012 - Operations Manager Databases](#)

- [Backup and Recovery Using VSS Writer](#)

Recommended Backup Schedule for System Center 2012 - Operations Manager

You should determine how often and when to run backups. In general, you should perform database backups according to your company's backup policy.

Backup Schedule

The following table suggests a schedule for regular backups of your Operations Manager features. These suggestions are specific to your Operations Manager environment and are meant to complement other regularly scheduled backups in your environment.

You should schedule those backup jobs at a time that does not conflict with the schedule of the Operations Manager grooming tasks. The Operations Manager grooming jobs run on the Operations Manager database server and both read from and write to the database. Backing up the database during the same time might cause failures in the backup job, the grooming job, or both.

At a minimum, an incremental backup of the operational database should be performed on a daily basis. A complete backup should be performed on the operational database weekly. The master and msdb databases should be backed up any time a change occurs that affects either database, but you should back them up at least monthly.

Feature to back up	Full backup	Incremental backup
Operational database	Weekly	Daily
Data warehouse database	Monthly	Weekly
Reporting server	On a recurring basis, with the frequency depending on how often reports change in your organization, and every time after significant changes are made to report definitions (including additions, changes, and deletions).	Same as full backup
Audit Collection Services (ACS) database	Monthly	Weekly
Master database (Master)	Every time, after installing and configuring the Operations Manager database features and after making significant changes to logons or other security changes.	Per IT policies
Msdb database (Msdbdata)	After the initial installation and	After changing the scheduled

Feature to back up	Full backup	Incremental backup
	configuration of the Operations Manager database features.	Microsoft SQL Server Agent jobs that Operations Manager uses.
Custom Management Packs (.xml files)	Monthly or after making significant changes to management packs.	Not applicable

How to Back Up Custom Management Packs

Management packs contain monitoring rules for applications and services. Both sealed and unsealed management packs can be customized by superseding their default values using overrides, or by defining custom rules or monitors. Custom management packs are unsealed and are saved to a separate .xml management pack file. Only custom management packs can be exported. By default, the file is saved to the My Default management pack folder.

You should back up custom management packs regularly even though backing up the operational database captures management pack information. When you run management pack backups as an independent operation from database backups, you can re-import them separately from the database, which can be useful in cases when you must roll back the customized changes in one or more custom management packs.

Use the Export feature from the Operations console to back up management packs.

To export a custom management pack

1. Log on to a management server with an account that is a member of the System Center 2012 – Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click **Administration**.
3. In the **Administration** pane, click **Management Packs**.
4. Right-click the custom management pack that you want to export, and then click **Export Management Pack**.
5. In the **Save As** dialog box, type the path and file name for the management pack file, or click **Browse** to save the file to a different directory, and then click **Save**.

How to Schedule Backups of System Center 2012 - Operations Manager Databases

Schedule a Database Backup

Use this procedure to schedule a database backup by using Microsoft SQL Server Management Studio to back up the operational database, the Audit Collection Services (ACS) database, and the data warehouse database.

► **To schedule a database backup to a file**

1. Start SQL Server Management Studio.
2. In the **Connect to Server** dialog box, select the appropriate values in the **Server type** list, in the **Server name** box, and in the **Authentication** box.
3. Click **Connect**.
4. In **Object Explorer**, expand **Databases**.
5. Right-click the database that you want to back up, click **Tasks**, and then click **Back Up**.
6. In the **Back Up Database** dialog box, type the name of the backup set in the **Name** box, and then under **Destination**, click **Add**.
7. In the **Select Backup Destination** dialog box, type a path and a file name in the **Destination on disk** box, and then click **OK**.

 **Important**

The destination location must have enough available free disk space to store the backup files based on the frequency of your backup schedule.

8. In the **Script** list, click **Script Action to Job**.
9. If you want to change job parameters, in the **New Job** dialog box, under **Select a page**, click **Steps**, and then click **Edit**.
10. Under **Select a page**, click **Schedules**, and then click **New**.
11. In the **New Job Schedule** dialog box, type the job name in the **Name** box, specify the job schedule, and then click **OK**.

 **Note**

If you want to configure alerts or notifications, you can click **Alerts** or **Notifications** under **Select a page**.

12. Click **OK** and **OK**.

Operational Database

The operational database contains almost all of the System Center 2012 – Operations Manager environment configuration settings, agent information, management packs with customizations, operations data, and other data required for Operations Manager to operate correctly.

 **Important**

It is critical that you back up the operational database regularly to preserve the latest information about your Operations Manager environment. A database failure without a recent backup results in the loss of almost all Operations Manager-specific data, and you would have to rebuild the entire Operations Manager environment.

 **Note**

If your backup procedure sets the operational database to be offline during backup, Operations Manager caches incoming data, and then, after backup is completed, Operations Manager stores that data in the database.

Reporting Databases

Operations Manager Reporting uses the following databases:

- Operations Manager data warehouse (data warehouse database)
- SQL Server Reporting Services databases (ReportServer and ReportServerTempDB)

The data warehouse database contains all of the performance and other operational data from your Operations Manager environment. SQL Server Reporting Services then uses this data to generate reports such as trend analysis and performance tracking.

To be able to restore reporting functionality in case of failure, it is critical that you back up the data warehouse database. When determining how often and when to back up this database, you should consider the following:

- This database can grow to a very large size (more than one terabyte) over time.
- Management servers frequently write data to this database.
- IT SLA requirements are based on the requirement for reporting availability in the organization.



Note

The data warehouse database uses a simple recovery model, which truncates all transactions after completion. Therefore, backing up only the log file is insufficient; you must back up the entire database.

The SQL Server Reporting Services databases store report definitions, report metadata, cached reports, and snapshots. In case of failure, you can re-create report definitions by re-importing the reports. However, cached reports, which are reports that have already been created, will be lost.

To be able to restore reporting functionality in case of failure, we recommend that you back up the SQL Server Reporting Services databases.

ACS Database

The Audit Collection Services (ACS) database, OperationsManagerAC, is the central repository for events and security logs that are collected by ACS forwarders on monitored computers.

The Audit Collection Services database can grow significantly depending on how many ACS forwarders send events to the ACS database and the filters configured to control what events are written to the database.

Master Database

The master database is a system database, which records all of the system-level information for a Microsoft SQL Server system, including the location of the database files. It also records all logon accounts and system configuration settings. The appropriate functionality of the master database is key to the operation of all of the databases in an instance of SQL Server.

MSDB Database

The MSDB database, Msdbdata, is a SQL Server system database, which is used by the SQL Server agent to schedule jobs and alerts and for recording operators. The appropriate functionality of the MSDB database is key to the operation of all the databases in an instance of SQL Server.

**Note**

This database contains task schedules that are vital to the health of the Operations Manager database, and it should be included in your backup plan. You have to back up this database only after you configure Operations Manager or if you change the scheduled agent jobs.

Backup and Recovery Using VSS Writer

With System Center 2012 Service Pack 1 (SP1), Operations Manager, VSS writers offer a shortcut for backing up the Operations Manager and Audit Collection Services databases using the SQL VSS writer, providing an alternative mechanism of selecting what to be backed up, versus using the user interface in Data Protection Manager (DPM) or some other application to select the SQL databases. Backup and restoration can be accomplished with DPM or any other backup application because we employ a generic VSS Writer.

The writer IDs are:

- Audit Collection Service: 2488ec56-996a-4716-8165-7436a683
- Operations Manager: 5ACDEAFF-4A8C-4FCE-BB24-BFCB4CD8A572

The VSS writers make it easy to discover what databases to backup, showing all the SQL data being used by Operations Manager and Audit Collection Service under the respective nodes.

**Note**

For Disaster recovery you need to follow the instructions at [Disaster Recovery in System Center 2012 - Operations Manager](#) with VSS writer based recovery.

**Note**

You must have local administrative credentials to back up and restore Operations Manager and ACS data stores.

Disaster Recovery in System Center 2012 - Operations Manager

Various System Center 2012 – Operations Manager servers and features can potentially fail, impacting Operations Manager functionality. The amount of data and functionality lost during a failure is different in each failure scenario. It depends on the role of the failing feature, the length of time it takes to restore the failing feature, and on the availability of backups.

You should always keep a backup of your operational database and data warehouse database. For information about scheduling regular backups of the Operations Manager databases, see [How to Schedule Backups of System Center 2012 - Operations Manager Databases](#).

The amount of data and functionality lost during a failure is different in each failure scenario. The impact of failure is minimized if the Operations Manager deployment includes multiple management servers. The impact is greater if only one management server is implemented. This is because you do not have a second management server which can take on the load if one fails, and you will lose all monitoring capabilities. The impact of failure of a management server in a distributed environment is minimized, but it increases the workload on additional management servers in the management group until the failed management server is restored.

Recovering Operations Manager Features

If your Operations Manager databases have failed, you can restore them from back up. For more information, see [How to Restore Operations Manager Databases](#).

If your Operations console, web console, or Reporting server have failed, you must reinstall them. For information on installing these features, see

- [How to Install the Operations Manager Web Console](#)
- [How to Install the Operations Console](#)
- [How to Install the Operations Manager Reporting Server](#)

If one or more management servers have failed, you can recover them by using the **setup.exe** command with a **/recover** switch in Command Prompt window. There are two scenarios for recovery. The first scenario is when you have to recover a management server when all management servers in the management group have failed. In this case, you must recover all of the failed management servers, and then reconfigure the RunAs accounts. The second scenario is when you have a failed management server, but one or more management servers are still online. In this case, you just recover all of the failed management servers. You should not reconfigure the RunAs accounts.

▶ To Recover a Management Server

1. Build a new server, ensuring that it meets the minimum supported configurations for System Center 2012 – Operations Manager, and use the same name that was given to the failed management server.
2. Restore the operational database and data warehouse database, if required. For more information, see [How to Restore Operations Manager Databases](#).
3. On the new server, open a Command Prompt window by using the Run as Administrator option, and run the following command:



Note

This process only recovers the management server. If consoles or Reporting were also installed on the failed management server, you must reinstall them after recovery is complete.



Important

You must use the same parameter values for account credentials, management group, and database names as the failed server you are trying to recover.



Important

The following command assumes that you specified the Local System for the Management server action account (`/UseLocalSystemActionAccount`) and Data Access service (`/UseLocalSystemDASAccount`). To specify a domain\user name for these accounts, you must provide the following parameters instead.

```
/ActionAccountUser: <domain\username> /ActionAccountPassword: <password>
```

```
/DASAccountUser: <domain\username> /DASAccountPassword: <password>
```

```
Setup.exe /silent /AcceptEndUserLicenseAgreement
/recover
/EnableErrorReporting:[Never|Queued|Always]
/SendCEIPReports:[0|1]
/UseMicrosoftUpdate:[0|1]
/DatabaseName:<OperationalDatabaseName>
/SqlServerInstance:<server\instance>
/DWDatabaseName:<DWDatabaseName>
/DWSqlServerInstance:<server\instance>
/UseLocalSystemDASAccount
/DatareaderUser:<domain\username>
/DatareaderPassword:<password>
/DataWriterUser:<domain\username>
/DataWriterPassword:<password>
/ActionAccountUser:<domain\username>
/ActionAccountPassword:<password>
```

Setup detects that the server was a prior management server in the management group, and recovers the management server. You must follow these procedures for each failed management server in your management group.

For information about the command-line parameters, see [Disaster Recovery Command-line Parameters](#).

If you have to recover a management server when all management servers in the management group have failed, then you must also reconfigure the RunAs Accounts.



Important

If you have management servers that have not failed, you should not reconfigure the RunAs Accounts.

▶ To Reconfigure the RunAs Accounts

1. In the Operations console, click the **Administration** button.
2. In the **Administration** pane, under **Run As Configuration**, click **Accounts**.
3. In the **Accounts** pane, right-click a Run As account, and then click **Properties**.
4. In the **Run As Account Properties** dialog box, click the **Credentials** tab.
5. Re-enter your credentials for the Run As account and click OK.
6. Repeat these steps for all Run As accounts.



Note

If you are not using SQL Server authentication, you can remove any associations to the **Data Warehouse SQL Server Authentication Account** and **Reporting SDK SQL Server Authentication Account** and then delete these accounts.

If you are not using SQL Server authentication, you can remove the SQL Server Authentication accounts.

► To Remove the SQL Server Authentication Accounts

1. In the Operations console, click the **Administration** button.
2. In the **Administration** pane, under **Run As Configuration**, click **Profiles**.
3. In the **Profiles** pane, right-click **Data Warehouse SQL Server Authentication Account**, and then click **Properties**.
4. Click **Run As Accounts** in the right pane, click **Data Warehouse SQL Server Authentication Account**, and then click **Remove**.
5. Click **Save**, and then click **Close**.
6. In the **Profiles** pane, right-click **Reporting SDK SQL Server Authentication Account**, and then click **Properties**.
7. Click **Run As Accounts** in the right pane, click **Reporting SDK SQL Server Authentication Account**, and then click **Remove**.
8. Click **Save**, and then click **Close**.
9. In the **Administration** pane, under **Run As Configuration**, click **Accounts**.
10. In the **Profiles** pane, right-click **Data Warehouse SQL Server Authentication Account**, and then click **Delete**.
11. In the **Profiles** pane, right-click **Reporting SDK SQL Server Authentication Account**, and then click **Delete**.

See Also

[Backup and Disaster Recovery in Operations Manager](#)

[Disaster Recovery Command-line Parameters](#)

Disaster Recovery Command-line Parameters

You can recover one or more management servers by using the **setup.exe** command in the Command Prompt window.

Command-line Parameters

The following table lists the command-line parameters for recovering an System Center 2012 – Operations Manager management server.

Note

If the parameter contains a colon, a value is required. Otherwise, it is simply a switch.

Parameter	Value
/silent	Required parameter. Runs the installation wizard without displaying the user interface
/recover	Recovers a management server.
/ManagementGroupName:	Optional. The name of the management group
/SqlServerInstance:	The SQL server and instance (<server\instance>).
/DatabaseName:	The name of the Operational database.
/DWSqlServerInstance:	The data warehouse server and instance (<server\instance>).
/DWDatabaseName:	The name of the data warehouse database.
/UseLocalSystemActionAccount	Used to specify the Local System for the Management server action account.
/ActionAccountUser:	The domain and user name of the Management server action account. Used if you do not want to specify the Local System
/ActionAccountPassword:	The password for the Management server action account. Used if you do not want to specify the Local System.
/UseLocalSystemDASAccount	Used to specify the Local System for the Data Access service account.
/DASAccountUser:	The domain and user name of the Data Access service account. Used if you do not want to specify the Local System.
/DASAccountPassword:	The password for the Data Access service account. Used if you do not want to specify the Local System.
/DataReaderUser:	The domain and user name of the data reader account.
/DataReaderPassword:	The password for the data reader account.

Parameter	Value
/DataWriterUser:	The domain and user name of the data writer account.
/DataWriterPassword:	The password for the data writer account.
/EnableErrorReporting:	Never: Do not opt in to sending automatic error reports. Queued: Opt in to sending error reports, but queue the reports for review before sending. Always: Opt in to automatically send error reports.
/SendCEIPReports:	0 : Do not opt in to the Customer Experience Improvement Program (CEIP). 1 : Opt in to CEIP.
/UseMicrosoftUpdate:	0 : Do not opt in to Microsoft Update. 1 : Opt in to Microsoft Update.
/AcceptEndUserLicenseAgreement	Used to specify that you accept the End User License Agreement (EULA).

See Also

[Disaster Recovery in System Center 2012 - Operations Manager](#)

How to Restore Operations Manager Databases

Use the following procedure to restore a System Center 2012 – Operations Manager database using Microsoft SQL Server Management Studio. This procedure applies to databases on SQL Server 2008 R2 and SQL Server 2008 R2 SP1.



Note

If you want to resize the operational database, you must resize it by using SQL Server. For more information, see [Microsoft SQL Server](#) in the TechNet Library.

► To restore a database backup

1. Start SQL Server Management Studio.
2. In the **Connect to Server** dialog box, select the appropriate values in the **Server type** drop-down combo box, in the **Server name** box, and in the **Authentication** box.
3. Click **Connect**.
4. In **Object Explorer**, expand **Databases**, and then select the **OperationsManager**, **OperationsManagerAC**, or **OperationsManagerDW** database.

5. Right-click the database, point to **Tasks**, and then click **Restore**.
6. Click **Database** to open the **Restore Database** dialog box.
7. On the **General** page, the name of the restoring database appears in the **To database** list.
8. In the **To a point in time** text box, either retain the default (**the most recent possible**) or select a specific date and time by clicking the browse button, which opens the **Point in Time Restore** dialog box.
9. To specify the source and location of the backup sets to restore, click the **From Device** option.
10. Click **Browse** to open the **Specify Backup** dialog box.
11. In the **Backup media** list box, select one of the listed device types. To select one or more devices for the Backup location list box, click **Add**.
12. In the **Select the backup sets to restore** grid, select the backups to restore. This grid displays the backups available for the specified location.
13. In the **Restore options** panel, select the **Overwrite the existing database** option.
14. In the **Restore the database files as** options panel, verify the original database file name and path are correct.
15. For the **Recovery state** options, specify the state option **Leave the databases ready to use by rolling back the uncommitted transactions**. Additional transaction logs cannot be restored.
16. Click **OK** to restore the database.

Making Changes to an Operations Manager Environment

After the initial deployment of System Center 2012 – Operations Manager, you might need to make changes or upgrades to the original deployment for reasons such as the following:

- You need to replace hardware that is experiencing problems and that is no longer considered reliable.
- You need to replace hardware as part of the upgrade process from System Center Operations Manager 2007 R2.
- You need to add additional hardware to improve scalability and performance.
- You need to move a database and log file to a different volume because of space or performance reasons.
- You need to change hardware that is leased and is due to expire soon.
- You need to change or upgrade hardware to comply with new hardware standards.
- You initially installed multiple Operations Manager features on a single server and you need to distribute some components to other servers.
- You need to restore functionality in a failure scenario.

Operations Manager supports changes to your Operations Manager infrastructure as listed below. Be cautious when performing these operations because they can result in data loss if not performed correctly.

- [Account Information for Operations Manager](#)
- [How to Uninstall Operations Manager](#)
- [How to Manage the Report Server Unattended Execution Account](#)
- [How to Configure the Internet Proxy Settings for a Management Server](#)
- [How to Move the Operational Database](#)
- [How to Move the Data Warehouse Database](#)
- [How to Move the Audit Collection Database](#)
- [How to Move the Reporting Server Role](#)
- [How to Remove the Management Server Role](#)
- [Removing a Gateway Server from a Management Group](#)
- [How to Remove Certificates Imported with MOMCertImport](#)

See Also

[Maintaining the System Center 2012 - Operations Manager Infrastructure](#)

Account Information for Operations Manager

During the setup and operation of System Center 2012 – Operations Manager, you are asked to provide credentials for several accounts. This section provides information about the various accounts and how to change the credentials or passwords for the accounts after a deployment.

- [Action Accounts](#)
- [Service Accounts](#)
- [Agent Installation Account](#)
- [Data Warehouse Write Account](#)
- [Data Reader Account](#)

Action Accounts

The Operations Manager management server, gateway server, and agent, all contain a process called MonitoringHost.exe. MonitoringHost.exe is used to accomplish monitoring activities, such as running a monitor or a task. For example, when an agent subscribes to the event log to read events, it is the MonitoringHost.exe process that runs those activities. The account that a MonitoringHost.exe process runs as is called the action account. The action account for the MonitoringHost.exe process that is running on an agent is called the agent action account. The action account used by the MonitoringHost.exe process on a management server is called the management server action account. The action account used by the MonitoringHost.exe process on a gateway server is called the gateway server action account.

When you validate or change the default action account, you must ensure that the account you are using for your default Action Account is configured to be a **Role** member of the **ConfigServiceMonitoringUsers** database role.

▶ To validate the Action Account

1. On the server that hosts the operational database, open SQL Server Management Studio and connect to the local server.
2. Expand **Databases**, and then expand the operational database, which by default is **OperationsManager**.
3. Expand **Security**, then **Roles**, and then **Database Roles**.
4. Verify that the **ConfigServiceMonitoringUsers** role is listed.
5. If this role is not listed, you can right-click **Database Roles** to add it.

Agent Action Account

Unless an action has been associated with a Run As profile, the credentials used to perform the action are those defined for the action account. For more information about the Run As profile, see [Managing Run As Accounts and Profiles](#). Some examples of actions include the following:

- Monitoring and collecting Windows event log data
- Monitoring and collecting Windows performance counter data
- Monitoring and collecting Windows Management Instrumentation (WMI) data
- Running actions such as scripts or batch files

MonitoringHost.exe is the process that runs these actions by using the credentials specified in the action account. A new instance of MonitoringHost.exe is created for each account.

Using a Low-Privileged Account

When you install Operations Manager, you can choose one of two options while assigning the action account:

- Local System
- Domain or Local Account

A common approach is to specify a domain account, which allows you to select a user with the least amount of privileges necessary for your environment.

The default action account must have the following minimum privileges:

- Member of the local Users group
- Member of the local Performance Monitor Users group
- Allow log-on-locally permission (SetInteractiveLogonRight)

The minimum described above are the lowest privileges that Operations Manager supports for the action account. Other Run As accounts can have lower privileges. The actual privileges required for the Run As accounts depend on which management packs are running on the computer and how they are configured. For more information about which specific credentials are required, see the appropriate management pack guide.

Keep the following points in mind when choosing credentials for the agent action account:

- A low-privileged account is all that is necessary for agents that are used to monitor domain controllers.
- Using a domain account requires you to update your password consistent with your password expiration policies.
- You must stop and then start System Center Management service if the action account has been configured to use a low-privilege account and this account was added to the required groups while the System Center Management service was running.

Notification Action Account

The notification action account is a Run As account that is created by the user to configure notifications. This is the action account that is used for creating and sending notifications. Ensure that the credentials you use for this account have sufficient rights for the SMTP server, instant messaging server, or SIP server that you will use for notifications.

If you change the password for the credentials that you entered for the notification action account, you have to make the same password changes for the Run As account.

Managing Action Account Credentials

For the account you choose, Operations Manager determines what the password expiration date is and generates an alert 14 days before the account expires. When you change the password in Active Directory, you can change the password for the action account in Operations Manager on the **Account** tab on the **Run As Account Properties** page. For more information about managing the action account credentials, see [How to Change the Credentials for the Action Account](#).

Service Accounts

The set of credentials of the System Center Configuration service and System Center Data Access service account is used by the System Center Data Access service and System Center Management Configuration service to update and read information in the operational database. Operations Manager ensures that the credentials used for the Data Access Services (DAS) service account are assigned to the Sdk_user role in the operational database. The System Center Configuration service and System Center Data Access service account can be configured as either a Local System account or as a domain account. A local User account is not supported.

If the management server and the operational database are on different computers, the System Center Configuration service and System Center Data Access account have to be changed to a domain account. For better security, we recommend that you use an account different from the one used for the management server action account. To change these accounts, see [How to Change Credentials for the System Center Management Configuration service and System Center Data Access service](#).

Agent Installation Account

When implementing discovery-based agent deployment, you are prompted for an account with administrator rights. This account is used to install the agent on the computer, and therefore it must be a local administrator on all the computers you are deploying agents to. The management server action account is the default account for agent installation. If the management server

action account does not have administrator rights, select **Other user account** and type an account that has administrator rights. This account is encrypted before it is used and then discarded.

Data Warehouse Write Account

The Data Warehouse Write account writes data from the management server to the Reporting data warehouse and reads data from the operational database. The credentials that you supply for this account are made a member of the roles according to the application, as described in the following table.



Note

For information about supported configurations for System Center 2012 – Operations Manager, see [Supported Configurations for Operations Manager for System Center 2012](#).

Application	Database/Role	Role/Account
Supported versions of Microsoft SQL Server	Operational database	db_datareader
Supported versions of Microsoft SQL Server	Operational database	dwsync_user
Supported versions of Microsoft SQL Server	Data warehouse database	OpsMgrWriter
Supported versions of Microsoft SQL Server	Data warehouse database	db_owner
Operations Manager	User role	Operations Manager Report Security Administrators account
Operations Manager	Run As account	Data Warehouse Action account
Operations Manager	Run As account	Data Warehouse Configuration Synchronization Reader account

If you change the password for the credentials that you entered for the Data Warehouse Write account, you have to make the same password changes for the following accounts:

- Run As account called Data Warehouse Action account
- Run As account called Data Warehouse Configuration Synchronization Reader account

Data Reader Account

This account is used to deploy reports, define what user the SQL Server Reporting Services uses to run queries against the Reporting data warehouse, and for the SQL Server Reporting Services

IIS Application Pool account to connect to the management server. This account is added to the Report Administrator User profile.

The credentials that you supply for this account are made a member of the roles according to the application, as described in the following table.



Note

For information about supported configurations for System Center 2012 – Operations Manager, see [Supported Configurations for Operations Manager for System Center 2012](#).

Application	Database/Role	Role/Account
Supported versions of Microsoft SQL Server	Reporting server installation instance	Report Server Execution Account
Supported versions of Microsoft SQL Server	Data warehouse database	OpsMgrReader
System Center 2012 – Operations Manager	User role	Operations Manager Report Security Administrators
System Center 2012 – Operations Manager	User role	Operation Manager Report Operators
System Center 2012 – Operations Manager	Run As account	Data Warehouse Report Deployment account
Internet Information Services (IIS)	Application pool	ReportServer\$<INSTANCE>
Windows Service	SQL Server Reporting Services	Log on account

If you change the password for the credentials that you entered for the Data Reader account, you have to make the same password changes for the following accounts:

- Report Server Execution Account
- The SQL Server Reporting Services service account on the computer that is hosting SQL Server Reporting Services (SSRS)
- The IIS ReportServer\$<INSTANCE> Application Pool account
- Run As account called Data Warehouse Report Deployment account

Account Information

- [How to Change the Credentials for the Action Account](#)
- [How to Change Credentials for the System Center Management Configuration service and System Center Data Access service](#)
- [How to Change IIS ReportServer Application Pool Account Password](#)

- [How to Change the Reporting Server Execution Account Password](#)
- [How to Change the Windows Service Account Password for the SQL Server Reporting Service](#)
- [How to Change the Run As Account Associated with a Run As Profile](#)

How to Change the Credentials for the Action Account

During the installation of System Center 2012 – Operations Manager, you are prompted for credentials for the management server action account. If you want to change the password for the credentials that you provided or use a different set of credentials, use the following procedure.

► To change the credentials for the action account

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the **Administration** pane, under the **Run As Configuration**, click **Accounts**.
4. In the **Accounts** pane, under **Type: Action Account**, right-click the account (domain\user name) that you want to change, and then click **Properties**.
5. In the **Run As Account Properties** dialog box, click the **Credentials** tab.
6. Enter the new credentials for the action account, and then click **OK**.

See Also

[Making Changes to an Operations Manager Environment](#)

[How to Change Credentials for the System Center Management Configuration service and System Center Data Access service](#)

How to Change Credentials for the System Center Management Configuration service and System Center Data Access service

During the installation of System Center 2012 – Operations Manager, you are prompted for credentials for the System Center Configuration service and System Center Data Access service. If you want to change the password for the credentials that you provided or use a different set of credentials, use the following procedure.



Note

The same credentials must be used for both services.

► To change credentials or password for the System Center Configuration service and System Center Data Access service

1. On the computer hosting the management server, on the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **services.msc**, and then click **OK**.
3. In the list of services, right-click **System Center Data Access Service**, and then click

Properties.

4. In the **System Center Data Access Properties** dialog box, click the **Log On** tab.
5. Enter new credentials or change the password of the existing credentials, and then click **OK**.
6. In the list of services, right-click **System Center Management Configuration**, and then click **Properties**.
7. In the **System Center Management Configuration Properties** dialog box, click the **Log On** tab.
8. Enter new credentials or change the password of the existing credentials, and then click **OK**.
9. Stop and restart both the **System Center Data Access** service and **System Center Management Configuration** service.

See Also

[Making Changes to an Operations Manager Environment](#)

[How to Change the Credentials for the Action Account](#)

How to Change IIS ReportServer Application Pool Account Password

If you change the password for the account that you specified as the Data Reader account during the setup of the System Center 2012 – Operations Manager Reporting server, you must change the IIS Report Server Application Pool account password. You can accomplish this by using the following procedure on the computer that is running SQL Server Reporting Services.

To change the IIS ReportServer Application Pool account

1. On the computer running SQL Server Reporting Services, on the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In **Internet Information Services (IIS) Manager**, expand **<Computer Name> (local computer)**, expand **Application Pools**, right-click **ReportServer<INSTANCE>**, and then click **Properties**.
3. In the **ReportServer<INSTANCE> Properties** dialog box, click **Identity**.
4. In the **Password** box, type the new password, and then click **OK**.
5. Close Internet Information Services (IIS) Manager.

See Also

[Account Information for Operations Manager](#)

[How to Change the Reporting Server Execution Account Password](#)

[How to Change the Windows Service Account Password for the SQL Server Reporting Service](#)

How to Change the Reporting Server Execution Account Password

If the password changes for the account that you specified as the Data Reader Account during the setup of the Reporting server, use the following procedure to change the Execution account password on the Reporting server.

► To change the Reporting Server Execution account password

1. On the computer hosting the Reporting server, on the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008 R2**, point to **Configuration Tools**, and then click **Reporting Services Configuration**.
2. In the **Reporting Server Installation Instance Selection** dialog box, click **Connect**.
3. In the **Reporting Services Configuration Manager** pane, in the left pane, click **Execution Account**.
4. In the **Execution Account** pane, type the new password for the execution account.
5. Click **Apply**, and then click **Exit** to close Reporting Services Configuration Manager.

See Also

[Account Information for Operations Manager](#)

[How to Change IIS ReportServer Application Pool Account Password](#)

[How to Change the Windows Service Account Password for the SQL Server Reporting Service](#)

How to Change the Windows Service Account Password for the SQL Server Reporting Service

If the password changes for the account that you specified as the Data Reader account during the setup of the Reporting server, use the following procedure to change the Windows service account for the SQL Server Reporting Services password on the computer running SQL Server Reporting Services (SSRS).

► To change the Windows service account for the SQL Server Reporting Services

1. On the computer running SQL Server Reporting Services, on the Windows desktop, click **Start**, point to **Settings**, and then click **Run**.
2. In the **Run** dialog box, type **services.msc**, and then click **OK**.
3. In **Services**, scroll down the list, right-click **SQL Server Reporting Services (<INSTANCE>)**, and then click **Properties**.
4. In the **SQL Server Reporting Services (<INSTANCE>) Properties** dialog box, click **Log On**.
5. In the **Password** and **Confirm Password** boxes, type the new password, and then click **OK**.
6. Close **Services**, and then close **Administrative Tools**.

See Also

[Account Information for Operations Manager](#)

[How to Change IIS ReportServer Application Pool Account Password](#)

[How to Change the Reporting Server Execution Account Password](#)

How to Change the Run As Account Associated with a Run As Profile

By default, the following Run As profiles have a Run As account associated with them.

- Data Warehouse account
- Data Warehouse Configuration Synchronization Reader account
- Data Warehouse Report Deployment account
- Data Warehouse SQL Server Authentication account
- Reporting SDK SQL Server Authentication account

For example, the Run As profile named Data Warehouse SQL Server Authentication account has the Run As account named Data Warehouse SQL Server Authentication account associated with it. As an example, you can use the following procedure to change the Run As account associated with the Run As profile called Data Warehouse SQL Server Authentication account. It is assumed that the new Run As account that you want to associate with this Run As profile has already been created. For more information about Run As accounts and Run As profiles, see [Managing Run As Accounts and Profiles](#)

► To change the Run As account associated with a Run As profile

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the System Center 2012 – Operations Manager management group.
2. In the Operations console, click the **Administration** button.



Note

When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager management server that you want the Operations console to connect to.

3. In the **Administration** pane, expand **Administration**, expand **Security**, and then click **Run As Profiles**.
4. In the Run As profiles pane, right-click **Data Warehouse SQL Server Authentication Account**, and then click **Properties**.
5. In the **Run As Profile - Data Warehouse SQL Server Authentication Account** dialog box, and then click the **Run As Accounts** tab.
6. Under **Run As Accounts**, click the targeted computer, and then click **Edit**.
7. In the **Edit Alternate Run As Account** dialog box, click the **Run As Account** list, select the new Run As account that you want to associate with this Run As profile, and then click **OK**.
8. In the **Run As Profile - Data Warehouse SQL Server Authentication Account** dialog box, click **OK**.

See Also

How to Uninstall Operations Manager

Use the following procedure to uninstall any feature of System Center 2012 – Operations Manager, including the management server, gateway server, Reporting server, operations console, web console, and agent.

▶ To uninstall System Center 2012 - Operations Manager

1. Log on to the server with an account that has local administrator rights.
2. In Control Panel, click **Programs and Features**.
3. On the **Uninstall or change a program** page, right-click **System Center 2012 - Operations Manager**, and then select **Uninstall/Change**.



Note

When you uninstall a stand-alone feature, the name that appears in **Program and Features** reflects the name of the feature.

4. On the **Getting Started, What do you want to do?** page, click **Remove a feature**. The Setup Wizard then identifies and lists all the features and roles that are installed on the local computer.
5. Select the features that you want to remove, and then click **Uninstall**.
6. On the **Complete, Component removal is complete** page, click **Close**.

See Also

[Making Changes to an Operations Manager Environment](#)

How to Manage the Report Server Unattended Execution Account

The System Center 2012 – Operations Manager Report Server unattended execution account is used to query data from the Reporting Data Warehouse. Users that manage this account require only the Read user right. This account is not managed from within the Operations Manager user interface. Use this procedure to change the user name or password for this account.

▶ To manage the Report Server unattended execution account

1. On the Windows desktop, click **Start**, point to **Programs**, point to **Microsoft SQL Server 2008 R2 SP1**, point to **Configuration Tools**, and then click **Reporting Services Configuration**.
2. In Reporting Services Configuration Manager, in the **Report Server Installation Instance Selection dialog** box, click **Connect**.
3. In the navigation pane, click **Execution Account**.
4. In the Execution Account pane, type a new user name or password as required.
5. Click **Apply**, and then click **Exit**.

See Also

[Account Information for Operations Manager](#)

How to Configure the Internet Proxy Settings for a Management Server

Use the following procedure to configure the Internet proxy settings for a System Center 2012 – Operations Manager management server. You must configure these settings if features of Operations Manager are enabled that require the management server to communicate over the Internet. For example, you must configure these settings if the Client Monitoring feature of Operations Manager is configured to transmit or receive data from Microsoft.

► To Configure Internet Proxy Settings for a Management Server

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the Administration button.
3. In the Administration pane, expand **Administration**, expand **Device Management**, and then click **Management Servers**.
4. In the results pane, right-click the management server for which you want to view the properties, and then click **Properties**.
5. In the **Management Server Properties** dialog box, click the **Proxy Settings** tab.
6. On the **Proxy Settings** tab, select **Use a proxy server for communication with Microsoft** and then do the following:
7. Select **http://** or **https://** from the drop-down list, and type the name of the Internet proxy server in the **Address** text box.
8. Type the **Port** number, and then click **OK**.

See Also

[Making Changes to an Operations Manager Environment](#)

How to Move the Operational Database

After the initial deployment of System Center 2012 – Operations Manager, you might need to move the operational database from one Microsoft SQL Server-based computer to another.

This procedure requires Microsoft SQL Server configuration. You need to back up a database, restore a database, update a database table, add new Logins, and modify User Mapping settings for Logins. For more information, see [SQL Server documentation](#).

Operational Database Relocation

Use the procedure below to move the operational database to a different server.

► To move the operational database

1. Stop the Operations Manager services (System Center Data Access, System Center Management, and System Center Management Configuration) on all the management

servers in the management group.

2. Use Microsoft SQL Server Management Studio to create a full backup of the operational database. The default name is OperationsManager.

For more information, see [How to: Back Up a Database \(SQL Server Management Studio\)](#).

3. On the new SQL server, copy the backup file to a local drive or map a local drive to the folder that contains the backup file.
4. Optionally, on the original server that hosts the operational database, delete the operational database.
5. On the new server, use Microsoft SQL Server Management Studio to restore the operational database that you previously backed up.

For more information, see [How to: Restore a Database Backup \(SQL Server Management Studio\)](#).

6. Update the registry on each management server in the management group to refer to the new SQL Server-based computer.



Note

Before editing the registry, follow your organization's backup policies with regard to the registry.

- a. Log on to the management server with Administrator permissions.
- b. Click **Start**, select **Run**, type **regedit** in the **Open** box, and then click **OK** to start Registry Editor.
- c. Under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\System Center\2010\Common\Database**, double-click the name **DatabaseServerName**, and then change the value to the hostname of the SQL Server-based computer now hosting the operational database, and then click **OK** to save your change.



Note

If you are using a named instance of SQL Server, be sure to use the `ServerName\Instance` name format.

- d. Close the Registry Editor.
7. On each management server, edit the following file:

```
%ProgramFiles%\System Center 2012\Operations Manager\Server\ConfigService.config
```

In the `<Category>` tag named "Cmdb", change the value for `ServerName` to the name of the new SQL server.

8. Update the operational database with the new database server name.
 - a. Open SQL Server Management Studio.
 - b. Expand **Databases**, **OperationsManager**, and **Tables**.
 - c. Right-click **dbo. MT_Microsoft\$SystemCenter\$ManagementGroup**, and then click **Edit Top 200 Rows**.
 - d. Change the value in the **SQLServerName_6B1D1BE8_EBB4_B425_08DC_2385C5930B04** column to

- reflect the name of the new SQL Server-based computer.
- e. Save the change.
9. Update the operational database with the new database server name to specify the location of the Application Performance Monitoring tables.
 - a. Open SQL Server Management Studio.
 - b. Expand **Databases**, **OperationsManager**, and **Tables**.
 - c. Right-click **dbo. MT_Microsoft\$SystemCenter\$OpsMgrDB\$AppMonitoring**, and then click **Edit Top 200 Rows**.
 - d. Change the value in the **MainDatabaseServerName_5C00C79B_6B71_6EEE_4ADE_80C11F84527A** column to reflect the name of the new SQL Server-based computer.
 - e. Save the change.
 10. On the new server hosting the operational database, expand **Security**, then expand **Logins**, and then add the data writer account.

For more information, see [How to: Create a SQL Server Login](#).
 11. Also in **Logins**, add the action account.
 12. Also in **Logins**, add the Data Access Service (DAS) computer account, using the form "domain\computername\$".
 13. For the DAS computer account, add the following user mappings:
 - ConfigService
 - db_accessadmin
 - db_datareader
 - db_datawriter
 - db_ddladmin
 - db_securityadmin
 - sdk_users
 - sql_dependency_subscriber



Note

If an account has not existed before in the SQL instance in which you are adding it, the mapping will be picked up by SID automatically from the restored operations database. If the account has existed in that SQL instance before, you receive an error indicating failure for that login, although the account appears in **Logins**. If you are creating a new login, ensure the User Mapping for that login and database are set to the same values as the previous login:

DW Data Writer: apm_datareader, apm_datawriter, db_datareader, dwsynch_users

Action account: db_datareader, db_datawriter, db_ddladmin, dbmodule_users

DAS/Configuration account: ConfigService, db_accessadmin, db_datareader, db_datawriter, db_ddladmin, db_securityadmin, sdk_users,

sql_dependency_subscriber

If DAS/Configuration uses the LocalSystem account, specify computer account in form <domain>\<computername>\$.

14. Execute the following SQL commands on new Operations database instance:

```
sp_configure 'show advanced options',1  
reconfigure  
sp_configure 'clr enabled',1  
reconfigure
```

15. Run the following SQL query:

```
SELECT is_broker_enabled FROM sys.databases WHERE  
name='OperationsManager'
```

16. If the result of the preceding query was an **is_broker_enabled** value of 1, skip this step. Otherwise, run the following SQL queries:

```
ALTER DATABASE OperationsManager SET SINGLE_USER WITH ROLLBACK  
IMMEDIATE  
ALTER DATABASE OperationsManager SET ENABLE_BROKER  
ALTER DATABASE OperationsManager SET MULTI_USER
```

17. Start the Operations Manager services (System Center Data Access, System Center Management, and System Center Management Configuration) on all the management servers in the management group.

See Also

[Making Changes to an Operations Manager Environment](#)

[How to Move the Data Warehouse Database](#)

How to Move the Data Warehouse Database

After the initial deployment of System Center 2012 – Operations Manager, you might need to move the data warehouse database from one Microsoft SQL Server-based computer to another.



Caution

This procedure can result in data loss if it is not performed correctly and within a reasonable length of time of the failure. Ensure that you follow all steps precisely, without unnecessary delays between the steps.

This procedure requires Microsoft SQL Server configuration. You need to back up a database, restore a database, update a database table, add new Logins, and modify User Mapping settings for Logins. For more information, see [SQL Server documentation](#).

Data Warehouse Database Relocation Procedure

Use the procedure below to move the data warehouse database to a different system.

► **To move the data warehouse database**

1. Stop the Operations Manager services (System Center Data Access Service, System Center Management Service, System Center Management Configuration Service) on all management servers in the management group.
2. On the current Data Warehouse server, use SQL Server Management Studio to create a full backup of the data warehouse database. The default name is OperationsManagerDW. We recommend that you also back up the associated master database.

For more information, see [How to: Back Up a Database \(SQL Server Management Studio\)](#).

3. On the new SQL server, copy the backup file to a local drive or map a local drive to the folder that contains the backup file.
4. Optionally, on the current Data Warehouse server, delete the data warehouse database.
5. On the new Data Warehouse server, use SQL Management Studio to restore the operational database that you previously backed up.

For more information, see [How to: Restore a Database Backup \(SQL Server Management Studio\)](#).

6. On the server hosting the Operations Manager Reporting component, update the registry to refer to the new SQL Server-based computer.



Note

Before editing the registry, follow your organization's backup policies with regard to the registry.

- a. Log on to the management server with Administrator permissions.
 - b. Click **Start**, select **Run**, type **regedit** in the **Open** box, and then click **OK** to start Registry Editor.
 - c. Under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager3.0\Reporting**, double-click the name **DWDBInstance**, and then change the value to the hostname of the SQL Server-based computer now hosting the operational database, and then click **OK** to save your change.
 - d. Close the Registry Editor.
7. Start the System Center Data Access Service on the management server associated with the reporting server.
 8. On the management server associated with the reporting server, change the connection string.
 - a. Open a browser and go to the reporting webpage, http://localhost/reports_instancename.
 - b. Click **Show Details** and then click **Data Warehouse Main**.
 - c. Change the **Connection String** to contain the new data warehouse server name, and then click **Apply**.
 - d. Close the browser.

9. On the management server associated with the reporting server, change the connection string for AppMonitoringSource.
 - a. Open a browser and go to the reporting webpage, `http://localhost/reports_instancename`.
 - b. Click **Application Monitoring**, and then click **.NET Monitoring**.
 - c. Click **Show Details**, and then click **AppMonitoringSource**.
 - d. On the **AppMonitoringSource** page, click **Properties** and change **Connection string** to contain the new data warehouse main data source server name, and then click **Apply**.
 - e. Close the browser.
10. On the server hosting the operational database, update the OperationsManager database table.
 - a. Open SQL Server Management Studio.
 - b. Expand **Databases**, **OperationsManager**, and **Tables**.
 - c. Right-click **dbo. MT_Microsoft\$SystemCenter\$DataWarehouse**, and then click **Edit Top 200 Rows**.
 - d. Change the value in the **MainDatabaseServerName_2C77AA48_DB0A_5D69_F8FF_20E48F3AED0F** column to reflect the name of the new SQL Server.
 - e. Close SQL Server Management Studio.
11. On the server hosting the operational database, update the OperationsManager database for Application Performance Monitoring functionality.
 - a. Open SQL Server Management Studio.
 - b. Expand **Databases**, **OperationsManager**, and **Tables**.
 - c. Right-click **dbo. MT_Microsoft\$SystemCenter\$DataWarehouse\$AppMonitoring**, and then click **Edit Top 200 Rows**.
 - d. Change the value in the **MainDatabaseServerName_5C00C79B_6B71_6EEE_4ADE_80C11F84527A** column to reflect the name of the new SQL Server.
 - e. Close SQL Server Management Studio.
12. On the new data warehouse server, update the member database.
 - a. Open SQL Server Management Studio.
 - b. Expand **Databases**, **OperationsManagerDW**, and **Tables**.
 - c. Right-click **dbo. MemberDatabase**, and then click **Edit Top 200 Rows**.
 - d. Change the value in the **ServerName** column to reflect the name of the new SQL Server.
 - e. Close SQL Server Management Studio.
13. On the new server hosting the operational database, expand **Security**, then expand **Logins**, and then add the data writer account.

For more information, see [How to: Create a SQL Server Login](#).

14. Also in **Logins**, add the data reader account.
15. Also in **Logins**, add the Data Access Service computer account, using the form “domain\computername\$”.
16. For the Data Access Service (DAS) computer account, add the following user mappings:
 - db_datareader
 - OpsMgrReader
 - apm_datareader



Note

If an account has not existed before in the SQL instance in which you are adding it, the mapping will be picked up by SID automatically from the restored data warehouse database. If the account has existed in that SQL instance before, you receive an error indicating failure for that login, although the account appears in **Logins**. If you are creating a new login, ensure the User Mapping for that login and database are set to the same values as the previous login:

DW Data Writer: db_owner, OpsMgrWriter, apm_datareader, apm_datawriter

DW Data Reader: db_datareader, OpsMgrReader, apm_datareader

DAS/Config account: db_datareader, OpsMgrReader, apm_datareader

If DAS/Config uses the LocalSystem account, specify computer account in form “<domain>\<computername>\$”.

17. Start the Operations Manager services (System Center Management, System Center Data Access, and System Center Management Configuration) on all the management servers in the management group.

► **To verify a successful move of the data warehouse database**

1. Verify that you can successfully run a report from the console.
2. Ensure that the health state of all management servers in the management group are **Healthy**.

If the health state of any management server is **Critical**, open **Health Explorer**, expand **Availability - <server name>**, and then continue to expand until you can navigate to **Data Warehouse SQL RS Deployed Management Pack List Request State**. Check the associated events to determine if there is an issue accessing the data warehouse database.

3. Check operating system events:
 - a. Open the operating system's Event viewer. Navigate to **Event Viewer**, and then to **Operations Manager**.
 - b. In the **Operations Manager** pane, search for events with a **Source** of **Health Service Module** and a **Category** of **Data Warehouse**.

The move was successful if event number 31570, 31558, or 31554 exists.

There is an issue accessing the data warehouse database if event numbers 31563,

31551, 31569, or 31552 exists.

4. Check events in Operations Manager:
 - a. In the Operations console, select **Monitoring**.
 - b. Navigate to **Monitoring, Operations Manager, Health Service Module Events**, and then to **Performance Data Source Module Events**.
 - c. Search the **Performance Data Source Module Events** pane for events with a **Date and Time** that is later than the move.

There is a problem with the data warehouse database if events have a **Source** of **Health Service Module** and an **Event Number** of 10103.

How to Move the Audit Collection Database

After the initial deployment of System Center 2012 – Operations Manager, you might need to move the Audit Collection (OperationsManagerAC) database from one Microsoft SQL Server-based computer to another.

This procedure requires Microsoft SQL Server configuration. You need to back up a database, restore a database, and add a new Login. For more information, see [SQL Server documentation](#).

ACS Database Relocation

Use the procedure below to move the ACS database to a different server.

To move the ACS database

1. On the original Audit Collection database server, stop Operations Manager Audit Collection Service.
2. Use Microsoft SQL Server Management Studio to create a full backup of the ACS database. The default name is OperationsManagerAC. We also recommend you back up the master database.

For more information, see [Create a Full Database Backup \(SQL Server\)](#).

3. On the new SQL server, copy the backup file to a local drive or map a local drive to the folder that contains the backup file.
4. Optionally, on the original server that hosts the ACS database, delete the ACS database.
5. On the new server, use Microsoft SQL Server Management Studio to restore the ACS database that you previously backed up.

For more information, see [Restore a Database Backup \(SQL Server Management Studio\)](#).

6. On the new ACS database server, use SQL Management Studio to create a login for the ACS server, as follows:
 - a. In SQL Server Management Studio, navigate to **Security** and then to **Logins**. Right-click **Logins** and select **New Login**.
 - b. In the **Login name** box, enter the ACS server (the system on which the ACS service

- runs) in the format **domain\computername\$**.
- c. Under **Select a page**, click **User Mapping**.
- d. Under **Users mapped to this login**, select the ACS database (default: **OperationsManagerAC**), and then, under **Database role membership for**, select **db_owner**.
- e. Click **OK** to save your new account.

For more information, see [Create a Login](#).

7. Update the registry on ACS server to refer to the new ACS database server.



Note

Before editing the registry, follow your organization's backup policies with regard to the registry.

- a. Log on to the management server with Administrator permissions.
- b. Click **Start**, select **Run**, type **regedit** in the **Open** box, and then click **OK** to start Registry Editor.
- c. Under **HKEY_LOCAL_MACHINE\Software\ODBC\ODBC.INI\OpsMgrAC**, double-click the name **Server**, and then change the value to the hostname of the SQL Server-based computer now hosting the ACS database, and then click **OK** to save your change.



Warning

If you are using a named instance of SQL Server, be sure to use the `ServerName\Instance` name format.

- d. Close the Registry Editor.
8. On the server on which the ACS service is running, start Operations Manager Audit Collection Service.

How to Move the Reporting Server Role

You can move the System Center 2012 – Operations Manager Reporting server component to a new server, or reinstall the component on the original server.

During this move, Operations Manager stops storing data in the OperationsManagerDW database until you complete the Operations Manager reporting server reinstall.

Use the procedures in this topic to move the reporting server to a new server and verify the success of the move. You must back up any custom reports that were authored outside of Operations Manager 2007. For more information about this, see [Moving the Report Server Databases to Another Computer](#) in the SQL Server 2008 Books Online (<http://go.microsoft.com/fwlink/?LinkId=151513>).



Note

Ensure that you follow all steps precisely, as not doing so might result in data corruption.

► **To move the Operations Manager reporting server**

1. Use Microsoft SQL Server Management Studio to create a full backup of the data warehouse database. The default name is OperationsManagerDW.
For more information, see [Create a Full Database Backup \(SQL Server\)](#).
2. On the current Operations Manager reporting server computer, uninstall the Operations Manager reporting server component as follows:
 - a. Click **Start**, click **Control Panel**, and then click **Add or Remove Programs** if you are using Windows Server 2003, or click **Programs and Features** if you are using Windows Server 2008.
 - b. In the **Add or Remove Programs** or **Programs and Features** dialog box, select **System Center 2012 - Operations Manager**, and then click **Uninstall/Change**.
 - c. In the **Operations Manager Setup** wizard, click **Remove a feature**.
 - d. In the **Select features to remove** page, select **Reporting server**, and then click **Uninstall**. Click **Close** when the wizard finishes.
3. On the new SQL server, copy the backup file to a local drive or map a local drive to the folder that contains the backup file.
4. Optionally, on the original server that hosts the operational database, delete the data warehouse database.
5. On the new server, use Microsoft SQL Server Management Studio to restore the data warehouse database that you previously backed up.
For more information, see [Restore a Database Backup \(SQL Server Management Studio\)](#).
6. If you are reinstalling the Operations Manager reporting server component on the original server, you must remove any data that is left from the original installation by doing the following:
 - a. Copy the ResetSRS.exe tool from the SupportTools folder on the product CD to a local folder.
 - b. Open a command prompt window using the **Run as Administrator** option and run the tool as follows:

```
ResetSRS.exe <SQL Server instance name>
```
 - c. Here, SQL Server instance name is the SQL Server instance that SQL Reporting Services is installed on, such as 'Instance1'. If SQL Server is using the default instance, enter MSSQLSERVER.
 - d. Open the Reporting Configuration Manager by clicking **Start**, pointing to **Programs**, pointing to **Microsoft SQL Server 2005** or **Microsoft SQL Server 2008**, pointing to **Configuration Tools**, and then clicking **Reporting Services Configuration**.
 - e. For SQL Reporting Services 2005, in the **Configure Report Server** page, check the status of the **Web Service Identity** item. If the status is not **Configured** (green), click that item, and then click **Apply**.
Check the status of the rest of the items on that page. Configure any items that are

designated with a red 'X', indicating an unhealthy configuration status.

7. On the new Operations Manager reporting server computer, install the Operations Manager Reporting server component as follows:
 - a. On the **Configuration, SQL Server instance for reporting services** page, make sure the **SQL Server instance** refers to the restored database.
 - b. On the **Configuration, Configure Operation Manager accounts** page, be sure the **Data Reader** account is the same account previously used for the Report server.

For more information, see [How to Install the Operations Manager Reporting Server](#).

Verify that you can successfully run a report from the Operations console.

Ensure that the health state of all **Management servers** is **Healthy**.

How to Remove the Management Server Role

Use the following procedure to remove the management server role from a computer. For example, you might have to do this if you have to reassign a computer that is hosting the management server role and install a gateway server.

Before you remove the management server role from a computer, you must configure any objects that are managed by that management server, to be managed by a different management server as described in the following sections.

The high-level steps to remove a management server role are as follows:

1. [Delete the Management Server](#) from the management group.
2. If the management server you are about to remove functions as a primary management server for an agent, you must configure those agents to use a new primary management server. See [Change the Primary Management Server](#).
3. If the management server you are about to remove acts as a proxy agent for an agentless-managed computer, you must identify a new management server. See [Configure an Agentless-Managed Computer to Use a Different Proxy Agent](#).
4. If the management server you are about to remove acts as a proxy agent for a network device, you must identify a new management server. See [Configure a Network Device to Use a Different Operations Manager 2012 Proxy Agent](#).
5. Remove the management server role from a computer. See [Remove the Management Server from a Computer](#).

Delete the Management Server

Use the following procedure to delete a management server role from the management group.

To delete a management server from the management group

1. Open the Operations console with an account that is a member of the Operations Manager Administrator role for the management group.
2. In the Operations console, click the **Administration** button.

**Note**

When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager management server that you want the Operations console to connect to.

3. In the **Administration** pane, click **Management Servers**.
4. Right-click the desired management server, and then click **Delete**.
5. In the **Confirm Delete Management Server** dialog box, click **Yes**.

Change the Primary Management Server

Use the following procedure to change the primary management server for agent-managed computers that are assigned to primary and secondary management servers without using Active Directory Domain Services.

► To change the primary management server for agent-managed computers by using the Operations console

1. Open the Operations console with an account that is a member of the Operations Manager Administrator role for the management group.
2. In the Operations console, click the **Administration** button.

**Note**

When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager management server that you want the Operations console to connect to.

3. In the **Administration** pane, expand **Administration**, expand **Device Management**, and then click **Agent Managed**.
4. In the **Agent Managed** pane, select the computers for which you want to change the primary management server, right-click them, and then select **Change Primary Management Server**.

**Note**

The **Change Primary Management Server** option is unavailable if Active Directory Domain Services was used to assign any of the selected computers to the management group.

5. In the **Change Management Server** dialog box, select the desired management server in the list, and then click **OK**. The change takes effect on the agent after its next update interval.

If you are changing the primary management server for a Linux or UNIX computer, the certificate that was used to access the Linux or UNIX computer must also be copied to the new management server. You do not have to copy the certificate if you are changing the primary management server for computers that are running Windows.

▶ **To copy a certificate from one server to another server**

1. Log on to the management server that has the certificate that you want to copy.
2. At the command prompt, change the directory to %ProgramFiles%\System Center 2012 – Operations Manager. Run the following command: **scxcertconfig.exe – export <filename>**.
3. While the file created by scxcertconfig.exe contains only the public key of the certificate, you should still treat it as a security-sensitive file. The file, and any copies of the file, should be explicitly deleted when the certificate is imported into the new management server in step 5 in this procedure. Verify that the new management server can access the file copy location.
4. Log on to the management server that you want to monitor agents from.
5. At the command prompt, change the directory to %ProgramFiles%\System Center 2012 – Operations Manager. Run the following command: **scxcertconfig.exe –import <filename>**.

The imported certificate is required for Operations Manager to trust agents signed with that certificate. If multiple management servers are signing certificates, the certificates must be exported from each management server, and imported to the other management servers.

Configure an Agentless-Managed Computer to Use a Different Proxy Agent

Use the following procedure to change the Operations Manager proxy agent for an agentless-managed computer. The proxy agent can be any agent-managed computer in the management group that is configured to be a proxy.

▶ **To change the proxy agent for agentless-managed computers**

1. Open the Operations console with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click the **Administration** button.



Note

When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager management server that you want the Operations console to connect to.

3. In the **Administration** pane, expand **Administration**, expand **Device Management**, and then click **Agentless Managed**.
4. In the **Agentless Managed** pane, select the agentless-managed computers for which you want to change the proxy agent, right-click them, and then select **Change Proxy Agent**.
5. In the **Change Proxy Agent** dialog box, select the computer that you want to be the new proxy agent, and then click **OK**.

Configure a Network Device to Use a Different Operations Manager 2012 Proxy Agent

Use the following procedure to change the Operations Manager proxy agent for network devices. The proxy agent can be any agent-managed computer in the management group. It must have Simple Network Management Protocol (SNMP) installed, an optional Windows element, and be able to connect to the devices that use SNMP.

► To change the proxy agent for network devices

1. Open the Operations console with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click the **Administration** button.



Note

When you run the Operations console on a computer that is not a management server, the **Connect To Server** dialog box appears. In the **Server name** box, type the name of the Operations Manager management server that you want the Operations console to connect to.

3. In the **Administration** pane, expand **Administration**, expand **Device Management**, and then click **Network Devices**.
4. In the **Network Devices** pane, select the network devices for which you want to change the proxy agent, right-click them, and then select **Change Proxy Agent**.
5. In the **Change Proxy Agent** dialog box, select the computer that you want to be the new proxy agent, and then click **OK**.

Remove the Management Server from a Computer

Use the following procedure to remove a management server role from a computer.

► To remove a management server role from a computer

1. In Control Panel, click **Programs and Features** on the computer from which you want to remove the management server component.
2. Right-click **System Center 2012 - Operations Manager**, click **Uninstall/Change**, and then follow the instructions in the wizard.

Removing a Gateway Server from a Management Group

Throughout the life cycle of your System Center 2012 – Operations Manager implementation, you might need to modify the structure and configuration of your deployment. In the case of gateway servers, these types of changes can stem from the decommissioning of an untrusted domain so that monitoring is no longer required or from the old server hardware being replaced with new hardware. To remove a gateway server from service, complete the following steps.

► Overview of Decommissioning a Gateway Server

1. Configure all objects that are being managed by the gateway server to use a different primary management server. For an agent-managed computer, this means using either another gateway server or a management server.
2. Uninstall the gateway server software from the server.
3. Delete the gateway server from the management group.

Configure Managed Objects to Use an Alternate Primary Management Server

Gateway servers can manage three different types of objects: agent-managed computers, agentless-managed computers, and network devices acting as a proxy agent.

► To configure agent-managed computers to use a different primary management server using the Operations console

1. Log on to a management server with an account that is a member of the Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the Administration pane, expand **Administration**, expand **Device Management**, and then click **Agent Managed**.
4. In the Agent Managed pane, select the computers for which you want to change the primary management server, right-click them, and then select **Change Primary Management Server**.



Note

The **Change Primary Management Server** option will be unavailable if Active Directory Domain Services was used to assign any of the selected computers to the management group.

5. In the **Change Management Server** dialog box, select the new management server from the list, and then click **OK**. The change takes effect on the agent after its next update interval.

Alternatively, this configuration can be changed on the agent-managed computer itself using either of the following two procedures.

► To change the primary management server for agent-managed computers by using the MOMAgent.msi setup wizard

1. Log on to the agent-managed computer with an account that is a member of the Administrators security group for the computer.
2. In **Add or Remove Programs**, click **Change** for **System Center Operations Manager 2012 Agent**.



Note

The **Agent Setup Wizard** can also be run by double-clicking MOMAgent.msi, which is located on the Operations Manager installation media.

3. In the **System Center 2012 – Operations Manager Agent Setup Wizard**, click **Next**.

4. On the **Program Maintenance** page, select **Modify**, and then click **Next**.
5. On the **Management Group Configuration** page, leave **Specify Management Group information** selected, and then click **Next**.
6. In the next **Management Group Configuration** page, do the following:
 - a. Type the name of the **Management Server**.
 - b. Type in a value for **Management Server Port**, or leave the default **5723**.
 - c. Click **Next**.
7. On the **Ready to Install** page, review the settings, and then click **Install** to display the **Installing the System Center 2012 - Operations Manager Agent** page.
8. When the **Completing the System Center 2012 - Operations Manager Agent Setup wizard** page displays, click **Finish**.

► **To change the primary management server for agent-managed computers using MOMAgent.msi from the command line**

1. Log on to the agent-managed computer with an account that is a member of the Administrators security group for the computer.
2. Open the command window.
3. At the prompt, run the following command:

```
%WinDir%\System32\msiexec.exe /i  
\\path\Directory\MOMAgent.msi /qn USE_SETTINGS_FROM_AD=0  
MANAGEMENT_GROUP=MG1 MANAGEMENT_SERVER_DNS=MS2.Domain1.net
```

This command reconfigures the agent to use **MS2.Domain1.net** as its primary management server for management group **MG1**.

 **Note**

Microsoft Windows Installer public properties must be uppercase, such as *PROPERTY=value*. For more information about Windows Installer, see [Windows Installer](#) in the Microsoft Developer Network library.

If the Domain Name System (DNS) and Active Directory names for the management server differ, the **MANAGEMENT_SERVER_AD_NAME** property also needs to be set to the fully qualified Active Directory Domain Services name.

Redirecting Agentless-Managed Computers and Network Devices

► **To change the proxy agent for agentless-managed computers and network devices**

1. Log on to a management server computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the Administration pane, expand **Administration**, expand **Device Management**, and then click **Agentless Managed**. If you are working with a network device, select **Device Management** and then **Network Devices**.

4. In the Agentless Managed pane, select the agentless-managed computers for which you want to change the proxy agent, right-click them, and then select **Change Proxy Agent**. Or if you are working with a network device, in the **Network Devices** pane, select the network devices for which you want to change the proxy agent, right-click them, and then select **Change Proxy Agent**.
5. In the **Change Proxy Agent** dialog box, select the computer you want to be the new proxy agent, and then click **OK**.

The final steps in removing a gateway server from a management group are straightforward:

- Log on to the gateway server with an account that has administrative rights.
- In **Add or Remove Programs**, select **System Center Operations Manager 2012 Gateway**, and then click **Remove**.

In the **Operations** console, in the **Administration** view, under **Device Management, Management Servers**, select the gateway server, right-click it, and then click **Delete**.

Deleting the Gateway Server

The final steps in removing a gateway server from a management group are straightforward:

- Log on to the gateway server with an account that has administrative rights.
- In **Add or Remove Programs**, select **System Center Operations Manager 2012 Gateway**, and then click **Remove**.

In the **Operations** console, in the **Administration** view, under **Device Management, Management Servers**, select the gateway server, right-click it, and then click **Delete**.

How to Remove Certificates Imported with MOMCertImport

Use the following procedure to remove certificates that have been imported using the MOMCertImport tool.

▶ To remove certificates imported with the MOMCertImport tool

1. Log on to the computer with an account that is a member of the Administrators group.
2. On the Windows desktop, click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **cmd**, and then click **OK**.
4. At the command prompt, type **<drive_letter>:** (where **<drive_letter>** is the drive where the System Center 2012 – Operations Manager installation media is located), and then press ENTER.
5. Type **cd\SupportTools\amd64** and then press ENTER.
6. Type the following:
MOMCertImport /Remove, and then press ENTER.

Sending Data to Microsoft

The following topics describe the different ways that you can send data to Microsoft to improve the products and features that you use most often and to help solve issues that you might encounter. Participation is voluntary, and the information is sent anonymously. You can opt in to any of the following programs.

Program	What it does	For more information
Customer Experience Improvement Program (CEIP)	Collects information about how you use Microsoft programs and about some of the issues that you might encounter.	Customer Experience Improvement Program (CEIP)
Operational Data Reporting	Collects a summary of how System Center 2012 – Operations Manager is being used and sends reports to Microsoft on a weekly basis. Microsoft uses these reports to improve the quality of its management packs and Operations Manager.	Operational Data Reporting (ODR)
Error Reporting	Anonymously sends reports of errors that occur in Operations Manager to Microsoft.	Error Reporting

See Also

[Maintaining the System Center 2012 - Operations Manager Infrastructure](#)

Customer Experience Improvement Program (CEIP)

The Microsoft Customer Experience Improvement Program (CEIP) collects information about how you use Microsoft programs and about some of the issues you might encounter. Microsoft uses this information to improve the products and features you use most often and to help solve issues. Participation in the program is strictly voluntary.

When you choose to participate in the CEIP, you configure clients with Group Policy to redirect CEIP reports to a System Center 2012 – Operations Manager management server, instead of reporting directly to Microsoft. The management servers are configured to forward these reports to Microsoft.

 **Important**

The CEIP reports do not contain contact information about you or your organization, such as names or an address.

The CEIP reports forwarded from your organization to Microsoft are combined with CEIP reports from other organizations and individual customers to help Microsoft solve issues and improve the Microsoft products and features that customers use most often. For more information about the CEIP, see [the CEIP page](#).

Use the following procedure to configure CEIP settings. The management server must have access to the Internet to participate in the program.

 **Important**

CEIP is a component of the Client Monitoring feature of Operations Manager. Client Monitoring must be enabled on at least one management server and managed computers to participate in the CEIP. For information about enabling the Client Monitoring feature of Operations Manager, see [Client Monitoring Using Agentless Exception Monitoring](#). After a management server has been configured for client monitoring, all agents that are participating in CEIP should be configured via Group Policy to send their CEIP data to that management server.

 **To configure the CEIP settings for Operations Manager**

1. Log on to a management server with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the **Administration** pane, expand **Administration**, and then click **Settings**.
4. In the **Settings** pane, expand **Type: General**, right-click **Privacy**, and then click **Properties**.
5. In the **Global Management Server Group Settings - Privacy** dialog box, on the **CEIP** tab, click **Join the Customer Experience Improvement Program (recommended)** to join the CEIP program or click **I don't want to join the program at this time** to decline participation. Then click **OK**.

 **Note**

You can click **Tell me more about the program** to view information about the CEIP program, including the privacy statement.

See Also

[Sending Data to Microsoft](#)

Operational Data Reporting (ODR)

The Microsoft Customer Experience Improvement Program (CEIP) collects information about how you use Microsoft programs and about some of the issues that you might encounter. Microsoft uses this information to improve the products and features you use most often and to help solve issues. Participation in the program is strictly voluntary.

During setup of System Center 2012 – Operations Manager Reporting, on the **Operational Data Reports** page, you have the option to join CEIP. If you elect to join CEIP, Operations Manager Reporting collects a summary of how Operations Manager is being used and sends reports to Microsoft on a weekly basis. Microsoft uses these reports to improve the quality of its management packs and Operations Manager. You can view the contents of these operational data reports (ODRs) by creating a Microsoft ODR Report.



Note

Before configuring operational data reports, make sure that Operations Manager Reporting is installed, and that the management server has access to the Internet so that reports can be sent to Microsoft.

▶ To configure the operational data reports settings

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the **Administration** pane, expand **Administration**, and then click **Settings**.
4. In the **Settings** pane, expand **Type: General**, right-click **Privacy**, and then click **Properties**.
5. In the **Global Management Server Settings - Privacy** dialog box, on the **Operational Data Reports** tab, click **Yes, send operational data reports to Microsoft (recommended)** to send reports or click **No, don't send operational data reports to Microsoft** to decline participation.
6. Click **OK**.

▶ To create a Microsoft ODR Report

1. Log on to the computer with an account that is a member of the Operations Manager Report Operators role for the Operations Manager management group.
2. In the Operations console, click the **Reporting** button.
3. In the **Reporting** pane, expand **Reporting**, and then click **Microsoft ODR Report Library**.
4. In the **Microsoft ODR Report Library Reports** pane, right-click one of the reports (for example, **Management Packs**), and then click **Open**.
5. In the Report view, in the **Parameter** area, click the Down Arrow in the **From** box, point to **This week**, and then click **Sunday**.
6. Click the Down Arrow in the **To** box, point to **This week**, and then click **Saturday**.
7. Click **Run** to display the ODR Report.
8. Click **Close** to close the report.

See Also

[Sending Data to Microsoft](#)

Error Reporting

When error reporting is enabled for System Center 2012 – Operations Manager features, if an error occurs, information about the error is anonymously reported to Microsoft. For more information about the privacy statement for the Microsoft Error Reporting Service, see [Microsoft Online Crash Analysis](#). This information is used with error reports from other Microsoft customers to help identify and resolve common issues with Operations Manager.



Note

This setting enables error reporting only for Operations Manager features. For information about enabling the Client Monitoring feature of Operations Manager, which includes error reporting for the specified computers, see [Client Monitoring Using Agentless Exception Monitoring](#).

► To configure error reporting settings

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the **Administration** pane, expand **Administration**, and then click **Settings**.
4. In the **Settings** pane, expand **Type: General**, right-click **Privacy**, and then click **Properties**.
5. In the **Global Management Server Settings - Privacy** dialog box, click the **Error Reporting** tab, and then do one of the following:
 - Select **Automatically send error reports about this product to Microsoft without prompting the user (recommended)**.
 - Select **Prompt the user for approval before sending error reports to Microsoft**.



Note

Click **Tell me more about error reporting** if you want to view the privacy statement for the Microsoft Error Reporting Service.

6. When you have made the selection that you want, click **OK**.

Error Transmission settings let you specify which error reports are sent to Microsoft and the additional diagnostic data that is included with the error reports.

► To find the Error Transmission tab of the Global Management Server Group Settings - Privacy dialog box

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
2. In the Operations console, click the **Administration** button.
3. In the **Administration** pane, expand **Administration**, and then click **Settings**.
4. In the **Settings** pane, expand **Type: General**, right-click **Privacy**, and then click **Properties**.

5. In the **Global Management Server Group Settings - Privacy** dialog box, click the **Error Transmission** tab.

**Note**

Click **Read the privacy statement** to view the privacy statement.

▶ To filter errors that are sent to Microsoft

1. On the **Error Transmission** tab of the **Global Management Server Group Settings - Privacy** dialog box, click **Filter**.
2. In the **Error Forwarding Filters** dialog box, select one or more of the options for sources of errors that you do not want forwarded to Microsoft, such as **that come from specific computers**.
3. In the **Criteria description** box, click **specific**, and provide the values for the criteria of errors that you do not want forwarded to Microsoft, such as **computer.contoso.com**.
4. Click **OK** twice.

▶ To configure diagnostic data sent to Microsoft with error reports

1. On the **Error Transmission** tab of the **Global Management Server Group Settings - Privacy** dialog box, do one or more of the following:
 - a. Select **Upload diagnostic data collection request**, select the additional diagnostic data that you want to send with error reports from computers that report errors to the management servers, and then forward them from the management server to Microsoft with the error reports.
 - b. Set **Maximum number of CAB files to send to Microsoft per error group** to help Microsoft diagnose the error. The recommended number is 10.
 - c. Select **Display links to solutions from Microsoft on error reporting computers**. A link to available solutions is displayed to end users after the error is first encountered and the link to the solution is downloaded to the management server.
 - d. Select **Display links to surveys from Microsoft on error reporting computers**.
 - e. Specify the **Default solution link when no Microsoft solution is available**. This can be an internal webpage for technical support, for example.
2. Click **OK**.

See Also

[Sending Data to Microsoft](#)